An evaluation of the security mechanisms within the Amazon S3 Cloud Platform.

Honours Project Final Report

Honours Project - (MHG405279)
Module Leader: Richard Foley

The Joker
BSc (Hons) Networking & Systems Support
Matric No: 20080xxxx

Project Supervisor: Prof. Huaglory Tianfield
Second Marker – Dr Richard Foley

“Except where explicitly stated all work in this document is my own”
Signed:______________________ Date:____________________

Abstract

Cloud Computing has been hailed as the future of data storage, however this technology is available today. Cloud computing is in essence, the storage of data and/or applications, out with the users local space. The contents of the ‘cloud’ are actually stored by a third party on their servers. The advantages of this service are the lack of overheads and cost saving to the user. Despite this however, the question arises how secure is the data the users entrust to this unseen, uncontrollable space? Despite a recent increase in popularity, the question of cloud content security weighs heavily on the early adopters and individuals yet to make the leap into the cloud.

This project, an ‘experimental’ type, will set out to evaluate the security of one of the most popular and typical cloud platforms, Amazon S3. In order to evaluate the security of this platform, several types of files including, photo, video, and PDF will be uploaded into the cloud. An experiment will be conducted on global storage buckets within Amazon S3 platform, to evaluate the security of these buckets against unauthorised access. Further testing will then be carried out on the various security mechanisms within Amazon S3, such as Bucket Polices and query-string authentication, to establish if these files are safe, or also vulnerable to unauthorized access.

The results of the experimental process will either show that unauthorised access can be achieved, or that the current security mechanisms offer an effective solution to protecting private data within the cloud. This project will be of significance to individual users of Amazon S3, as well as businesses contemplating embracing this technology as a whole, and could elevate fears of cloud computing security, which millions of user’s current harbour.

Acknowledgements

I would like to thank my supervisor Dr Huaglory Tianfield for his time, advice and guidance throughout this project.

I would also like to thank all my lecturers and tutors, which have taught me a great deal throughout my four years at Glasgow Caledonian University.

Extended thanks to all the great people I have met/worked with during my university career, especially in long two-hour lecturers.

Table of Contents

1. Introduction

The following sections will develop a background knowledge of cloud computing and the specific platform and security mechanisms which will be researched. General Cloud computing will be discussed including its development/history, its uses to both personal customers and home users and its potential for the future.

The specific cloud platform, Amazon S3, will be further discussed in order to build knowledge of its ability in order to evaluate it. This platform will also be compared with industry alternatives.

Other important aspects of the project will be developed including a research question, project aims, objectives to be achieved throughout, and possible hypotheses which will be tested and evaluated.

1.1 Background

1.1.1 Cloud Computing

Cloud Computing is becoming increasing popular in today's modern age of computing, however the concept of 'cloud' computing still mystifies many. "Clouds are all the rage today, promising convenience, elasticity, transparency, and economy"(Anthes,G. 2010). This view of cloud computing now becoming the must use technology, is a popular argument, "Touted by its advocates as the next big thing in computing" (Blumenthal,M. 2011).

The basic theory behind cloud computing is that the user stores their files, programs and other applications remotely. This means that computing and the access of the users data becomes more like a service, which can be accessed from any computer with Internet access. The storage of the user's data is trusted to a third parties server. "Cloud-storage providers offer users clean and simple file-system interfaces, abstracting away the complexities of direct hardware management" (Bowers, K.D. 2009).

This method of computing can have major advantages for both the individual user and businesses, for example, if the user's files and other data are no longer stored locally, then high capacity storage devices now become redundant. The financial benefits of this cloud method of storage are significant, as the reduction of overheads to businesses, and the saving of storage equipment and physical products to the individual home user highlights (Srinivasan,M. 2010). Not only are there financial benefits but cloud computing offers a new level of mobility to the computer user, as the user is not fixed to one computer to access their data or applications.

Cloud Computing presents opportunities to various users and organisations. Businesses, both small and large, are exploring the concept of cloud computing. There have become two different types of cloud, which are commonly used, public clouds and private clouds. A public cloud is the typical means of cloud computing where the user accesses their data and connects to their cloud provider using the Internet. A private cloud is generally for use in businesses, where the access is limited and controlled by the company and only employees of that business, or individuals with security permissions, can access the data or resources (Sehgal,N. 2011). Among the early developers of the cloud computing where Amazon and Google, who started developing there cloud services when the technology was still unknown. Other Organisations have started to explore the potential cloud based services could have, for example, as discussed in (Thomas,P.Y. 2011), the use of cloud computing services within the educational system and the class room itself, is being developed and could potentially change the current methods of teaching and learning.
The American Federal Government, not wishing to be left behind, is also aiming to move its data and resources into the cloud (Maitner,R., Jr,CGFM, PMP 2011), however this has provoked the reservations of many, as to the security of the data held within the cloud.

1.1.2 Cloud Security

The one key area of cloud computing which has held back its development and popularity in recent years is its security. "Security is one of the biggest challenges to the cloud model" (Hofmann,P. 2010). This aspect of data security within the cloud is important to both individual home users and business organisations that are looking to invest in the technology. One of the main concerns with cloud security is also the main components of the technology, the location of the data, how can a customer of a cloud based service have confidence in the security measures in place to protect their data (Mansfield-Devine,S. 2008). The fact that the data is under the control and supervision of a third party can be of concern to the data owner.

"Security plays a central role in preventing service failures and cultivating trust in cloud computing" (Khan,K. 2010). In order for potential users of cloud computing, who have reservations about security, to be convinced of its data protection, sufficient security mechanisms need to be in place to protect the files and applications the users upload or store on the cloud. The basic principle of cloud computing highlights security concerns to the user, however when multiple cloud providers and cloud services are also connected, the level of security must be higher and maintained to ensure that data is secure (Lakshminarayanan,S. 2010).

The information, which could be contained within this virtual 'cloud', could be highly confidential. As discussed in (Barnes,F., JD 2010), information management is becoming a part of the cloud revolution, with many organisations storing their information and records within a cloud environment. The medical profession is also embracing the technology, and storing confidential client records remotely in the cloud. A survey (Bowers,L. 2011) showed that over half of the pharmaceutical companies that took part in the survey, said that more than 11% of their IT budget, for the next three years, would be spent on cloud computing. Security of the cloud is such a large problem that the Cloud Security Alliance (cloudsecurityalliance.org) has been set up to advertise the best security procedures for cloud computing and computing in general.

There have been a number of high profile security lapses within cloud computing in recent years. Google Docs had an error concerning access control, which allowed unauthorized personnel to access documents that should have been protected. Amazon S3, which will be discussed below, had security issues when users could not access their files are there was an error with the file hash values (Popa, R.A. 2010). Protecting cloud services against hackers is a primary concern and must be addressed to give reassurance to users (Gold,S. 2010) however the user can help in protecting their data by regularly evaluating what they store on the cloud, this aids the service provider as there is less information to store and protect.

1.1.3 Amazon S3 Cloud Platform

One of the most popular cloud computing storage platforms is Amazon Simple Storage Service or Amazon S3 for short. This service allows users to upload their files to the cloud service (Amazon, 2012) in order to store their data and access it again at any time. Amazon S3 offers cloud storage that is scalable and reliable, at low cost to the user. All of Amazon’s own websites use S3 to store and run material. It is not just individual home users which benefit from this service as businesses can also use S3 to store data and/or the business website.

1.1.4 Security Mechanisms

Cloud based services use various security mechanisms in order to protect the data that they hold. One of the most common mechanisms is Access Control Lists, which provide authorisation to different users (Harnik, D,2009), this method also uses secret keys that the user shares with the service provider. Although this methods works in its basic form it is still vulnerable to attack, therefore further development has been undertaken to reinforce this method, “Cryptographic access control techniques designed for shared/untrusted file systems are potential candidates for clouds” (Zarandioon, S, 2010).

Amazon S3 has two mechanisms which are used to protect the files users upload to the cloud, these are; query string authentication and bucket policies. The query string authentication technique checks if the user, who is trying to access a file, is authorised or not before granting access. A Bucket within Amazon S3 is where the files and data are stored, and these buckets can have policies written to them that provide security for their contents.

This experimental project will assess the current level of security on the popular cloud-computing platform Amazon S3. The results of the experiments will show if the security mechanisms that are available to users, query string authentication and bucket policies, are sufficient enough in protecting the information and files users entrust to the platform. This paper will highlight any possible improvements that could be made to the platform in order to tighten security, and will allow for further research into cloud based file security.

1.2 Project Outline & Research Question

This following section will detail the project outline and the research question that the primary research and objectives will aim to develop. The overall aims and objectives will be discussed in greater detail and various hypotheses expressed and justified.

1.2.1 Project Overview

Cloud computing offers an attractive solution to customers keen to acquire computing infrastructure without large up-front investment (Bradshaw, S. 2011) Cloud computing is gaining popularity and is being used by not only business user but also the wider public. With individuals entrusting their data and file to this ‘cloud’ space, security of such data is of critical importance.

1.2.2 Project Type

This project will be an experimental project that has been developed in order to evaluate the security mechanisms available to protect user’s data, within the popular Amazon S3 cloud-computing platform. This project will aim to replicate the conditions the average user experiences, in order to establish if the content they upload to the cloud is protected or in fact vulnerable.

This research will show if Amazon S3, as a cloud platform, can be trusted with the content of its users and also highlight any further means of security open to the user.

1.2.3 Research Question

This project will aim to answer the following research question in detail:

“Are the current security mechanisms, including query string authentication and bucket polices, within the Amazon S3 cloud-computing platform, effective in protecting the data and files of its users?”

1.2.4 Aims and Objectives

The main aim of this project is to evaluate the security mechanisms within the Amazon S3 cloud-computing platform, in order to establish if the content stored within it is secure. This will be done by uploading content to the platform and testing its security features. Throughout this project there will be various objectives, highlighted from both secondary and primary research, which will help to reach the overall aim of the project.

The following objectives will be achieved through secondary research i.e. the literature review:

- Understand the methodology of 'Cloud' Computing

  In order to understand the project area research into the methodology of cloud computing will be essential.

- Understand security fears in relation to cloud computing

  Understanding the security fears commonly found with the cloud-computing concept will allow further discussion later in the project. This is also essential to the project topic.

- Analyse Amazon S3 cloud platform

  Gaining an understanding of the cloud platform will be important, as it is the environment that will be used throughout the project. It will also aid in reaching an overall conclusion and answering the research question.

- Understand security mechanisms, query string authentication, and bucket policies

  In order to evaluate the level of security within the cloud platform it is essential that an understanding of the current security mechanisms be reached.

- Identify other security mechanisms with could be adopted

  Analysis of other possible security measures, which could be adopted, could be valuable if the cloud platform is found to have a weakness in security.

The following objectives will be achieved through primary research:

- Creation of Amazon S3 account

The creation of an Amazon S3 account will allow for use of the cloud storage service, which will be used to upload files and test the security mechanisms that protect the data.

- Upload files of various types into the cloud storage

Files including, text files, picture files, and PDF files will be uploaded into the cloud platform. This will allow testing to be carried out on the accessibility of those files.

- Experiment with security mechanisms

The files stored on the cloud will be protected using two different security mechanisms; these will be query string authentication and bucket policies. Experimenting with these mechanisms will aid in the creation of test data.

- Testing of security with test data

Test data will be used in order to evaluate the security levels of the files stored on the platform. The results of this test data will be essential in arriving at a conclusion on the scrutiny of the platform, and in turn answer the research question.

- Testing of global amazon buckets with third party software

A third party program called ‘Bucket Finder’ will be used, as well as a word list, in order to evaluate the security of a vast number of public amazon S3 buckets and the files which reside within them.

1.3 Report Structure

The following section will give an overview of the rest of this report including the remaining chapters; Literature Review, Methods, Results and Discussion and Conclusions.

1.3.1 Literature Review

The second chapter in this report is the literature review that will develop a greater understanding of specific areas in relation to the overall project aim; this is done through secondary research.

The research starts with cloud computing in general including its methodology, primary concept and uses. As the research continues, the focus of attention will narrow in order to gain a greater knowledge of areas key to this project.

Research into cloud security in particular will be carried out, including detailed research into the specific security mechanisms that can be implemented within the Amazon S3 cloud platform. The findings of this research will build a platform from which the primary research will be carried out, and ultimately answer the research question.

1.3.2 Methods

The third chapter of this project discusses the main primary methods that will be used throughout the project. As this project is an experimental based project, multiple stages of the experiment will be detailed including a justification for each. This chapter will also provide detailed analysis of the experiment design, the equipment that will be used to carry out the experiment, the configuration of software used, and finally the procedure implemented in order to deliver a comprehensive experiment.

1.3.2 Results

Chapter 4 will detail the results of the experiment, which are outlined in section 3. This section will not only highlight the results which were found, but will also provide analysis and visual interpretation of what the experiments say about the security of the Amazon S3 cloud platform.

1.3.4 Discussion and Conclusions

The discussion and final conclusions detailed within section 5 will further analyse the results of the experiment process, while aiming to answer the overall research question. The sections will also highlight any possible future development of the project area. The final stage of this report will deliver the final summarised findings of the project and conclude the aims and questions the project sought to address.

2 Literature Review

The literature review is a valuable part of any project as it helps to build up knowledge of a specific area of interest. The overall goal of a literature review is to expand the understanding of a certain topic while using this knowledge to direct the rest of the projects focus. There are various useful sources of information for example, Academic Journals, developer websites, Conference papers, and also relevant books.

Literature Review objectives are as follows:

- Gain an understanding of the Cloud Computing Methodology
- Investigate common fears of Cloud Computing technology
- Investigate security mechanisms which are deployed within Clouds

2.1 Understanding of Cloud Computing Methodology

2.1.1 Server side Storage

Cloud Computing is essentially server side storage of a user's data and files. This is the key aspect of cloud computing, the content is not contained within the users own physical side, but rather stored at a company's own server farm. By moving their data to the cloud customers can avoid the costs of building and maintaining a private storage infrastructure, opting instead to pay a service provider as a function of its needs (Blandford,R. 2011). This method is called a Public cloud as the user is not able to directly control the data as the information is stored on a third parties server. However it has been reported within a study carried out by the Ponemon Institute that most cloud computing providers aren't all that concerned with their customers data security -- and even consider it the customers' responsibility to safeguard whatever data they store in the cloud (Anonymous 2011).

This principle of cloud storage methodology that the content uploaded to the cloud is actually located on a company's server is what cause potential users to worry about how safe their data actually is. Commercial clouds, such as Amazon S3, which will be discussed in detail throughout this project, have made cloud-computing solutions accessible to the wider public by offering different types of functions to the customer such as, services on demand, social networking and storage based solutions (Aljabre,Abdulaziz 2012). The cost advantages are the major positives to using cloud-based storage. Many major IT companies have invested vast amounts of money into building 'Server Farms' in order to deal with the future traffic that the ever-expanding cloud will bring.

Apple recently started development on their upgraded server farm in North Carolina at the expense of a reported $1 Billion Dollars, with this development solely aimed at their iCloud service. This huge sum of money invested by one of the biggest companies in the world, shows that cloud services/storage is the focus for the future, however are customers comfortable with their precision information being located in these far away servers.

Amazon were one of the first major IT powers to invest significantly into cloud computing, making their overall cloud platform *Amazon Web Services* into one of the biggest and most popular cloud solutions today. In order to protect the users data within the cloud, amazon states that, “objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region” (Amazon, 2012) this means that if the information is corrupt of lost within a server at one location then there will be a backup of that data at another amazon location, which will in turn be retrieved in case of emergency. This gives some insurance to users that if something goes wrong at the server side of storage; their important data will not be lost forever.

However is this enough protection for the user?

Despite the protection mentioned previously, the thought of information being duplicated and stored in multiple server locations could also be a cause for concern. How can the user be assured that all copies of the data are sufficiently protected?

2.1.2 Cloud Storage Services

Cloud storage is one particular aspect of cloud computing which has potentially vast benefits for both the home user and business. Cloud storage applications are available through a wide range of companies including, amazon and apple. Consumers relay on ‘cloud storage’ already even if they aren’t aware of it, for example whenever you update your status on Facebook, check your e-mail via Gmail, post your vacation photos on Flickr, or shop, bank, or play games online, you are relying on somebody else's computers to safeguard your information (Cachin,C. 2011)

Major companies to improve the services they already offer have already adopted cloud storage, however it's concept of using the cloud as the primary storage location for all the users’ data, which has not yet been realized. Security of data is essential for any user, with many cloud storage companies emphasizing their commitment to security.

- Dropbox

Dropbox is one of the most popular cloud storage services available to the public. It allows users to store various types of files within the cloud and also share them with other others of which they chose. Dropbox was originally released back in 2008 and offers both free and paid services. The free basic option of storage is 2GB, however it is possible to upgrade to a larger space allocation. Strategic Finance (Castelluccio,M. 2010) conducted research into the most popular cloud storage services, the first services on their list was Dropbox. One of the key points highlighted in this research was that Dropbox is a universal service, meaning its works on mac, pc and other popular platforms. Another interesting point raised within the paper is that Dropbox uses military grade encryption to protect the data throughout the transfer and storage process.

- iCloud

Apple is arguably the biggest and wealthiest company in the world. In 2011 they released their cloud service 'iCloud'. iCloud allows users to store various types of files including music, emails, contacts, and photos on the remote apple servers. As previously stated in this paper, apple has recently invested more than $1 Billion in the development of its server farm in North Carolina in order to support this cloud service. Once users have sent their data/files to the cloud, all the files are automatically synced to each of the users IOS devices or Mac computer. Similarly to Dropbox, iCloud comes with 5GB of free storage space; however customers can pay a premium for larger amounts of storage space.

- Amazon S3/ Amazon Web Services

Amazon S3 (Simple Storage Service) is the biggest and most comprehensive cloud storage platform available. First launched back in 2006, amazon has managed to establish this platform as the biggest and most popular of its kind. As discussed in a paper by the Association for Computing Machinery (Vogels,W. 2009), Amazon S3 is only one part of Amazon Web Services, which offers various other cloud computing solutions on a global scale. This research efficiently highlights the computing power at the heart of amazon cloud services, in fact figures show that there are more than 762 billion objects/files stored within the S3 platform. The basic methodology of S3 is that a user can upload files, known as objects, into buckets, which are storage space, where they have be stored and also accessed through URL or linked to web pages. Amazon S3 is used to host thousands of entire websites. The platform is used on such a massive scale that even other cloud storage companies, such as the fore mentioned Dropbox, have and still do use amazon's web services for their operations.

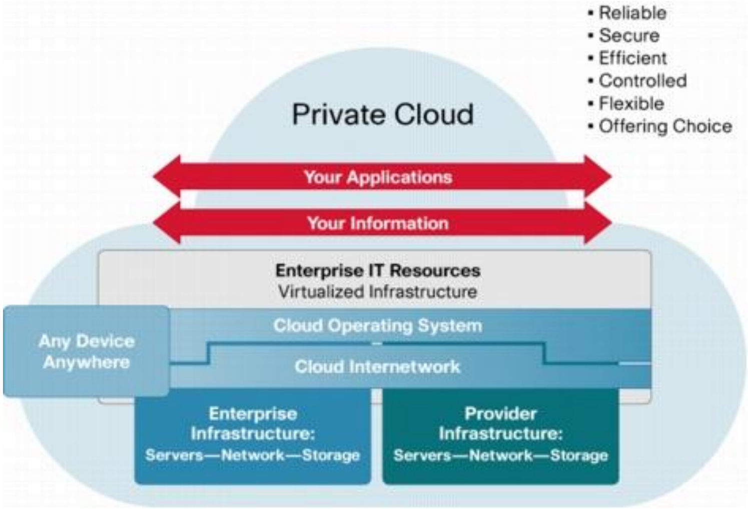
2.1.3 Cloud computing within business

Despite the large growth of cloud technology, if cloud computing is to become the industry standard for such things as storage, then more organisations must be convinced to take the leap into the cloud. The benefits for both small and large-scale businesses are real. "Online storage service providers grant a way for companies to avoid spending resources on maintaining their own in-house storage infrastructure and thereby allowing them to focus on their core business activities" (Das,S. 2011), this quote from a paper into risk management and optimal pricing highlights the major positive of cloud/internet based storage for any business. As long as the data is secure, which this paper will aim to answer, then there is no reason why a greater number of businesses should not adopt this method of storage.

There are many cloud options open to business leaders who wish to implement the technology within their organisation, for example private and public clouds.

- Private Cloud

Private clouds are best suited to large scale companies who wish to be able to control, design, develop and maintain the cloud within their premises (Wang,W. 2011). This form of internal cloud allows for greater security as the company itself is in direct control of the content within the cloud, the access rights of employees, the physical access to servers and other essential equipment.



(Figure 1, Example private cloud infrastructure, (Cisco, 2012))

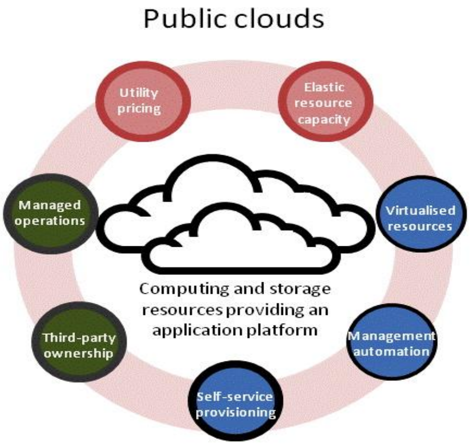
Research carried out by Business wire (Anonymous 2011) found that although there are risks involved in deploying a new technology within a company's infrastructure, there can be significant rewards in productivity, employee's personal development, and cost saving on physical equipment. Although many large-scale companies use the private form of cloud computing, what about the smaller business and the options open to them.

- Public Cloud

Research carried out by CMA Magazine (Stoller,J. 2011) states that cloud computing levels the playing field between small and large-scale companies. It is argued that through the use of public clouds, smaller companies can access the same huge levels of computing power and resources that larger organisations have at their disposal. The key methodology of a public cloud is that a service provider offers various resources such as storage, applications, and services, over the Internet.

As the user does not control the servers where the data is stored, the fear of data loss or corruption comes to the forefront of possible adopters minds. Amazon is the biggest of the public cloud service providers (Kabay,M E. 2011).

An interesting journal by Information Technology (Han,Y. 2011) into the costs of cloud computing deployment highlights the operational costs of using such cloud providers as Amazon and Google. Using case studies of the fore mentioned companies this paper delivers a breakdown of common applications and the overall cost to the companies that may use the service. The results showed that the start-up costs of such cloud platforms, as Amazon is a minimal fee compared to traditional methods of networking and storage. The major cost saving which is discussed through the paper is that of hardware. Due to the service provider being used within a public cloud, there are no hardware costs to the service user.


Public clouds
Utility pricing
Elastic resource capacity
Managed operations
Virtualised resources
Computing and storage resources providing an application platform
Third-party ownership
Management automation
Self-service provisioning

(Figure 2, Example of a public cloud and its characteristics, (MWDAdvisors, 2010).)

The *Information Management Journal* (Gable,J.,CRM, FAI, 2011) carried out research into the positives and negatives of cloud computing to small and large-scale businesses. The paper showed that although there are obvious advantages to the use of public cloud services, there are also drawbacks. The main issues highlights was the user knowledge of cloud computing, knowledge breeds confidence, yet there is still a naivety about the technology which holds individuals as well as companies executives from deploying cloud based infrastructures. The other main issue is security of data, which will be discussed in the following section.

2.2 Investigation into cloud security fears

2.2.1 Public opinion towards cloud security

Public fears of data integrity and non-authorised access have hindered the wide spread adoption of cloud computing, however this is slowly changing. Security is the number one concern for many users of cloud storage services and other cloud based services. Research into cloud security carried out by the IEEE Computer Society (Ren,K. 2012), discusses the potential security risks concerning cloud security. The paper mentions various security concerns such as, media failure, software issues, admin errors, and malicious hacking. However other possible security concerns are, the cloud service provider accessing users content without direction or consent, physical manipulation of equipment that the data is held on, all these threats are real to the consumer. It is the company's responsibility to put safe guards in place while also reassuring the customer that their data is safe.

One particular point of concern to the wider public is that with cloud based storage, data is stored in various different parts of the world, and despite this enabling a cost and performance benefit, the data could end up in a country which is without strong privacy laws or even none at all (Rose,C. 2011). Trust is something which consumers are being forced into; if they do not trust the cloud service provider to keep their data safe then they simply cannot use the services.

This concern of security from potential users of the service is what this project will aim to relieve. Using the biggest cloud storage service, Amazon S3, and conducting strict testing on the security mechanisms involved can assure sceptics of the service of its quality and strength.

Many have campaigned for public Audibility of cloud services. This method of publicly auditing the security procedures and methods of cloud computing companies has its positive arguments. A definition of public auditability, "a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed" (Wang,C. 2010). This governance would reassure users that the service provider is protecting their data, and a third party public auditor was working independently to ensure this (Wang, Q. 2011). One question that would still remain however would be who would be the pubic auditor? Can they themselves be trusted to work without any interference from providers?

Network Security (Walters,R. 2010) recently conducted research into the aspects of cloud computing which has put some users off or caused them concern. The physical access by employees of these cloud service providers, to the servers that hold the data the users entrust, was one of the major concerns. This research also supports the case for an independent company to regulate best practise for the cloud providers.

Worlds Governments have also started to embrace the technology but not without some reservations. A survey of federal government agencies in the United States (Anonymous 2010) found that 70% of all the agencies were concerned with data security within the cloud. Local government agencies were less concerned however, with 45% of local governments using a form of cloud computing already. It is believed that since this research was conducted back in 2010 another 20% of local government agencies are using cloud-based applications. These figures show that cloud computing solutions are growing in popularity however even the government of the largest power in the world has its concerns with cloud security.

2.2.2 Cloud Security Alliance

Although public auditing of cloud computing providers hasn't come to fruition yet, there is one organisation that has been formed to observe and regulate cloud-computing practise between the major providers. “The Cloud Security Alliance is the world's leading organization focused on the cloud, and has assembled top experts and industry stakeholders to provide authoritative information about the state of cloud security in the Cloud Security Alliance Summit.” (Anonymous 2010). Formed back in 2008, this non-profit organisation involved some of the biggest IT companies in the world including, Dell, Ebay, Sun, BT and Rackspace. The board of CSA consists of industry leaders, corporation and association figures and other stakeholders. CSA has produced white papers on various aspects of cloud security including, auditing databases, data protections, and virtualisation security.

This organisation allows members to join and help contribute to the network of cloud providers and solutions. There are sectors of the alliance in major countries around the world including the UK. The work carried out by the CSA helps to reassure individuals as well as businesses that cloud computing can be safe and help educate them in cloud computing practises.

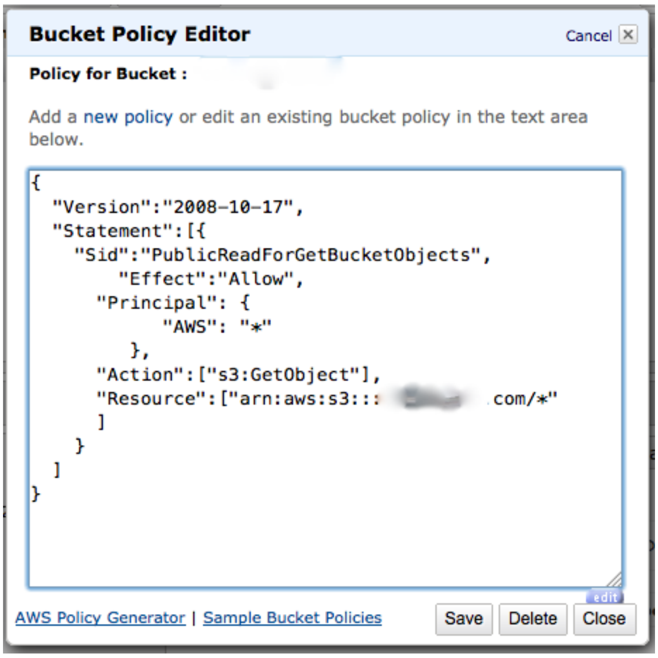
2.3 Investigation into Common cloud security mechanisms

2.3.1 Access Control List policies

Access control is the most important aspect of data security. Access control policies can be written to individual files/objects or as featured in Amazon S3 they can be written to buckets, forming Bucket Policies. The Computer Journal (Zhou,L. 2011) recently conducted research into a role based access mechanism for cloud storage where the data owner would encrypt the data and grant access to that encrypted data to users with specific roles. This means that personnel could only access data that is relevant to them. This method of access control highlights the need for such security precautions.

It could be dangerous for individuals or organisations to gain access to, for example, government files; this means that for data to be stored within the cloud, the level of access on each file or bucket must be set. Access control lists are not new to cloud computing, this form of security has been deployed in personal and business environments for years. With data in the cloud being duplicated in order to provide a backup if something goes wrong, the access control must be set over all known copies of that data.

Amazon S3 has made access control lists one of the main security precautions available to the consumer. Bucket policies have recently been added to the amazon s3 platform so that user can set access control policies for all the files within each bucket; this means that all the files that are contained in that bucket will share the overall buckets access policy. There are also various ways in which access can be restricted for example. Access can be limited to a specific HTTP referrer, Anonymous user, or an IP address.



Bucket Policy Editor

Policy for Bucket : [redacted]

Add a new policy or edit an existing bucket policy in the text area below.

```
{
  "Version":"2008-10-17",
  "Statement":[{
    "Sid":"PublicReadForGetBucketObjects",
        "Effect":"Allow",
      "Principal": {
            "AWS": "*"
         },
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3::: [redacted] .com/*"
      ]
    }
  ]
}
```

(Figure 3, Example of Amazon S3 Bucket Policy Editor)

Further research into cloud storage access (Kamara, S. 2010) has reiterated the need for such control of access and has also put forth arguments for Cryptographic storage including access control lists. Within this paper a process of quality checks on the files held in storage and that of the user that wishes to access the data, is carried out before a generator will grant access to the files.

2.3.2 Query String Authentication

Query string authentication another important security mechanism within Amazon S3, this allows HTTP or web browser access to files stored within the cloud which would normally need authentication/. The query string uses a signature in order to secure it and also requires an expiration date in order for the file to be made available. With this mechanism in place users can make the files they have stored within the cloud available to other users using a URL. The require recipient of the URL can use it to access the file as long as they have the correct permissions.

Research conducted by The Ohio State University (Switzer, D,2010) discussed the various security mechanisms available within Amazon S3 and in particular query string authentication. The paper highlighted that although this form of security allows the user to share files and these files are protected, they are not encrypted by amazon in fact amazon does not encrypt any of the files or data before they are stored with the cloud. This lack of encryption could allow for potential hacking, or unauthorised manipulation of data without the owner's consent. Amazon does however have a service called Amazon S3 Encryption Service, but this service is at the discretion of the user and not automatic.

The URL that will grant access to a bucket or file could look like the following example (Amazon Web Services, 2012):

http://quotes.s3.amazonaws.com/nelson?AWSAccessKeyId=44CF9SAMPLEF252F707&Expires=1177363698&Signature=vjSAMPLENmGa%2ByT272YEAiv4%3D

This example use of query string authentication contains three important URL parameters, Amazon Web Services Access Key, Expiration Date and Signature.

The two security mechanism which have been detailed above each protect against unauthorized access, which from the previous research and literature review materiel, is what the wider public are most concerned with in terms of cloud storage security.

3 Methods

This section of the report details the methods that will be carried out in order to evaluate the security mechanisms within the Amazon S3 cloud storage platform. The experimental approach to this project will be discussed and justified. This chapter will detail the equipment necessary to complete the experiment as well as the procedure used throughout.

3.1 Primary Research Method

The aim of this project is to evaluate the security mechanisms, access control policies and query string authentication, of the Amazon S3 cloud platform. The primary method for this research will be an experimental project. (Kajendran, K,2010) detailed that cloud storage services must be tested and evaluated in order to give the user confidence in them. The research approach from this paper on cloud storage is similar to this project however this project will focus specifically on Amazon S3 and its security mechanisms already in place. After reading this paper and other similar methods of research into cloud computing, the decision to carry out an experiment on the cloud platforms own security provisions would be most beneficial to the millions of consumers already relaying on those very security measures. The research which has been carried out throughout the literature review stage has supplied journals, work of researchers, detailed information on the security mechanisms and conclusions on how best to tackle the remain objectives in the project. This research will be particularly useful to the users of amazon S3, the developers of cloud storage services and businesses wishing to use this service, as it will determine if the data uploaded to the storage service is well protected or actually open to manipulation.

This research into the specific security mechanism within the Amazon S3 platform has not been conducted before; therefore this project cannot be directly compared to previous research in this area. The experiment will be a realistic one, which will not involve any simulation; therefore it will be able to deliver a better evaluation of the security users trust every day.

This experiment will involve checking the security of public storage buckets that already exist on the Amazon S3 platform. This research will show the effectiveness of the security that is currently protecting millions of buckets within the cloud service. By conducting part of the experiment process on publicly available buckets, the results will be as realistic as possible therefore meaning that the finding of this paper will be of particular interest to the customers of the service today.

By splitting the experiment process into different sub-experiments, the integrity of the data collected during each experiment will be maintained. There will be various different security mechanisms being evaluated during the experiment process, therefore it would be beneficial to conduct these evaluations separately.

3.2 Experiment to be conducted

This section provides detail into the nature of the experiments carried out in this project. The software and other equipment used through the experimentation process will be documented below.

3.2.1 Design and Equipment

As a result of the findings from the Literature Review, it became apparent that using the exact processes that everyday users of Amazon S3 carry out in order to place and protect their files on the service, must be followed during this experiment. However due to the various different aspects of the security being evaluated during this experimentation process, different approaches must be deployed for each security aspect.

The experiment will be carried out using an Apple computer, which has access to the Amazon Web Services website. It is within this website that the web browser interface of Amazon S3 can be used to upload, control and organise the files to be used in the experiment. This interface allows for uploading of the test files, as well as altering the security features so as they may be evaluated.

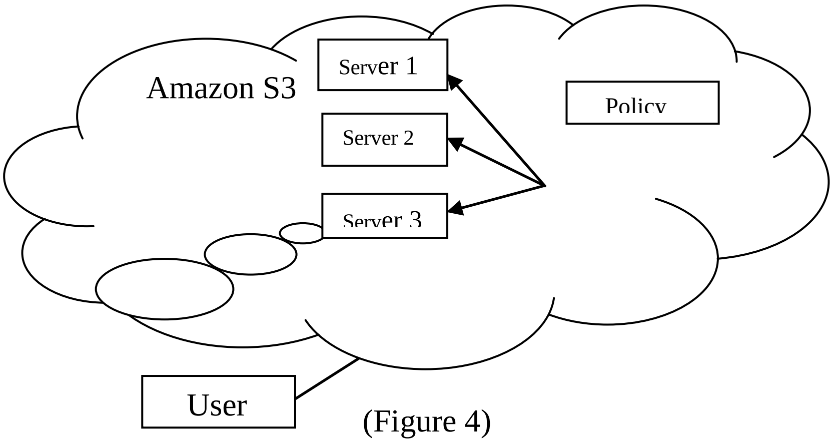
In order to effectively test the security of the service, a piece of third party software will be used which can establish if the test bucket is secure or accessible, this software will be used in a number of different ways throughout the experimental phase of the project in order to best evaluate the various aspects of security, both for the test bucket and test files but also to test the security of public buckets already used by Amazon S3 customers.

The third party software called ‘Bucket Finder’ is open sourced and is licenced under the Creative Commons Licencing laws. Consultation with the software developer has been made, with assurances in regards to the legality of the software having been delivered. This software is programmed using the ‘Ruby’ programming language and is compatible with the Apple computer the experiment will take place with.

The ‘Bucket Finder’ software will be used throughout all aspects of the experimentation phase. The first part of the experiment will involve the use of the software searching through the Amazon S3 database of storage buckets, to match any buckets with a given name, this will be explained in greater detail within the following sections, and display information regarding security access of both storage buckets and the files contained within the buckets. The second part of the experiment will involve applying an Access Control Policy to the test bucket, i.e. Bucket policy. This will then be tested using the Bucket finder tool to establish whether the bucket is secure and the access limitations within the policy are working, or if there is indeed a vulnerability within the security. The third aspect of the experiment will involve URL links being created for the test files, which again using the bucket finder tool, will be tested to establish if the Query string authentication mechanism efficiently protects the links to the test files, or if there is in fact a security vulnerability.

3.3 Implementation of Experiment

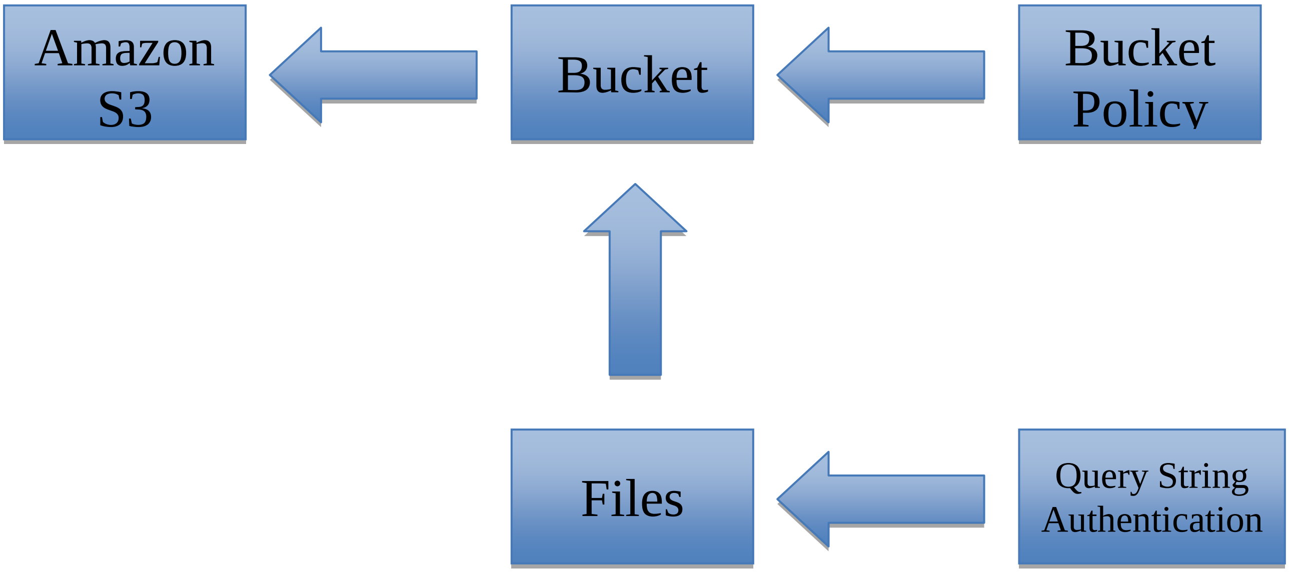
The Amazon S3 cloud storage service has a distinct architecture which is implemented in order to protect again data loss. Figure 4 below is a graphical representation of the S3 architecture. The user first uploads their files into a unique 'Bucket' which is used to store their files within the cloud. The files are subsequently duplicated, with each version sent to a different server location. This process aids data recovery in the event of data loss.



(Figure 4)

3.3.1 Security of Global Buckets

The main part of the experimentation stage of this project will be an investigation into the security of global buckets, which already exist. In order to conduct an experiment into this area of Amazon S3's security, a search will be carried out within the database of Amazons buckets in order to establish key security information on these real buckets. Figure 5 below shows how the bucket system employed within Amazon S3 works.



(Figure 5)

This experiment will use the aforementioned ‘Bucket Finder’ software tool. This tool provides a means by searching through the Amazon S3 cloud service to not only asses the security of individual test buckets which will be further assessed throughout this project, but also the buckets real life users of Amazon S3 use to store their data.

The first step in the experiment will be to construct a word list. One feature of Amazon S3 buckets is that all bucket names must be unique; therefore no two buckets can have the same name. With the use of a word list, it is possible to search throughout the Amazon cloud service to find unique real buckets, which match the names contained within the word list. As many buckets are used for personal use, individuals may find it practical to name their buckets after their own names. Therefore a word list will be constructed for use in this experiment, which will contain 943 different common names which people may have called their own Amazon storage buckets.

The next stage of the experiment is to load the wordlist into the Bucket finder tool, within the command line Terminal, so as the bucket finder can begin to search through all known amazon storage buckets to see if any buckets are registered under the names within the word list.

Once the bucket finder tool finds a match, it will display key information about the bucket it has found. The tool will highlight whether the bucket that has been found is public or in fact a private bucket. It is important to note that although this experiment will be searching through the names of real buckets, at no point will any private information be downloaded or disclosed. Instead the results of the experiment will show which of the buckets found are in fact publically accessible buckets. However despite these buckets being public, it could be possible that private information is contained within these public buckets without the user being aware that their private information is vulnerable to unauthorised readers.

The results of this experiment will show not only which of the buckets found are public or private, but will also show which files are contained within the buckets, and provide information on those files, for example, whether the files themselves are public or private, the URL link to the files location, and the types of files that are contained within these storage buckets.

3.3.2 Bucket Policy Access Control

One of the most recognised security mechanisms is called a Bucket policy, otherwise known as access control list. Once the test files have been uploaded, an access control policy will be generated in order to restrict access to unauthorised users and this will then be set to the test bucket containing the test files. The Bucket finder tool will once again be used to search for the test bucket within the Amazon S3 platform, the results of this experiment will display whether the bucket, with the policy applied, is displayed as public or private. The results will also show whether it is possible to see which files are stored within the test bucket despite the access policy having been applied to the bucket. These procedures will aim to answer; can the files be accessed by anyone regardless of authority? Can the files be downloaded without authority? Depending on results this will show if the bucket policies available to protect files work or if they are in fact weak and open to manipulation.

The effectiveness of the bucket policy will be of great importance, as it will show if it is possible for an unauthorised person to look within the bucket to see the files within, even though they might not have the ability to access the files. The ability to see the file names that are contained within private buckets could be enough to give unauthorised persons important information. This experiment, with the use of the bucket finder tool, will provide important results to the overall question of Amazons S3's security features.

Access control is an important aspect of security as discussed with (Yu, S. 2010) where the encryption techniques are detailed including pre proxy encryption. The policies and access rights discussed within this fore mentioned paper would aid in the experiment this project will carry out.

3.3.3 Query String Authentication

The next mechanism to be evaluated will be query string authentication. This procedure will require the creation of a URL in order to allow authorised users to access and/or download the file(s) from the amazon servers. The URL is protected using query string authentication, however this experiment will evaluate the security of this URL and determine if manipulation of this URL could lead to the access of the files. This phase of the experiment will again use the Bucket Finder software. Firstly the URL links to the test files will be created within the Amazon S3 interface.

Then using the Bucket Finder tool within the command line Terminal, a search will be carried out for the specific test bucket within the Amazon S3 service. The result of this search should show if the test files are public files or private files, from there the URL link will be displayed, that link will then be typed into an Internet browser.

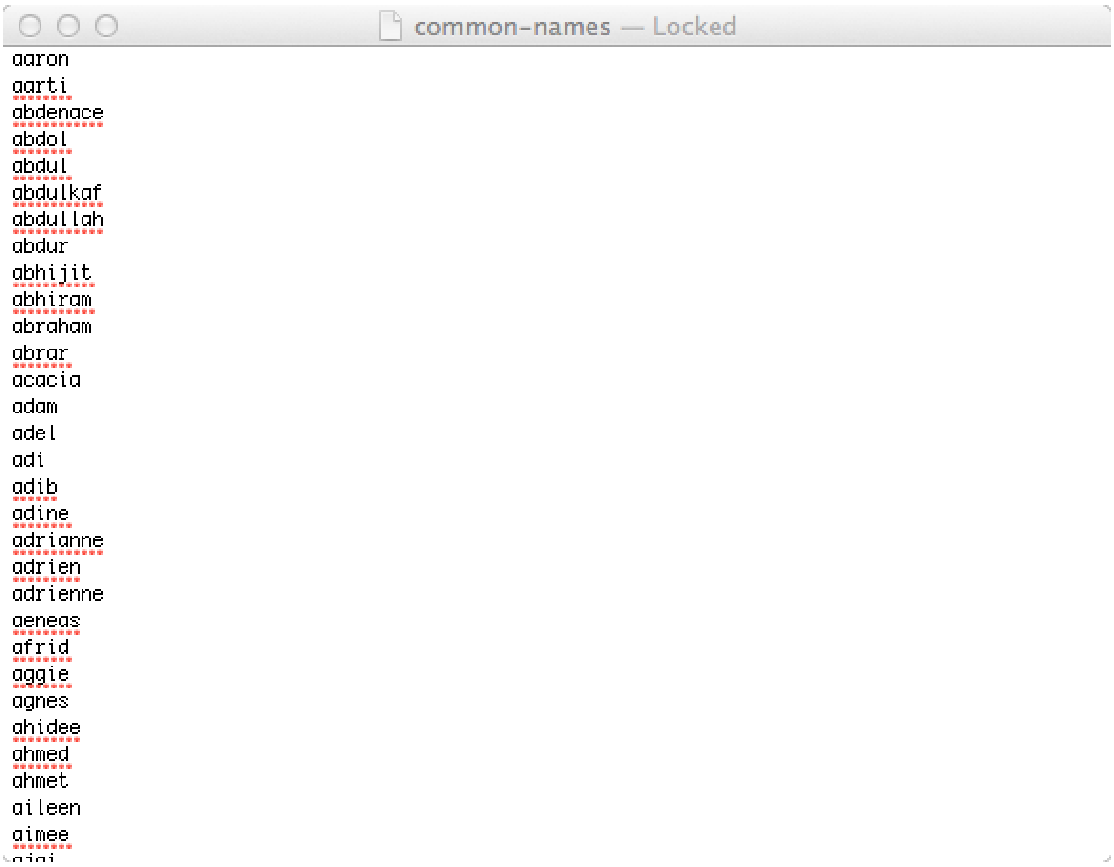
A test will then be carried out to see if access can be gained to the file using the URL link found within the Bucket Finder tools search. If the files can be access despite this security measure being in place, then it could possibly highlight a weakness in the security mechanism itself.

4 Results

This chapter of the project will present the results of the experiment, detailed in chapter 3. These results will be analysed and displayed with the aid of visual graphs etc., in order to answer the hypotheses and aims this paper set out to address.

4.1 Security of Global Buckets

The first stage of the experimental process was to assess the security of real global buckets used throughout the Amazon S3 service. This experiment started with a wordlist, which was used to search the database of buckets. Figure 6 below shows the list of common names that were used throughout this first phase of experiment.



```
aaron
aarti
abdenace
abdol
abdul
abdulkaf
abdullah
abdur
abhijit
abhiram
abraham
abrar
acacia
adam
adel
adi
adib
adine
adrianne
adrien
adrienne
aeneas
afrid
aggie
agnes
ahidee
ahmed
ahmet
aileen
aimee
aigi
```

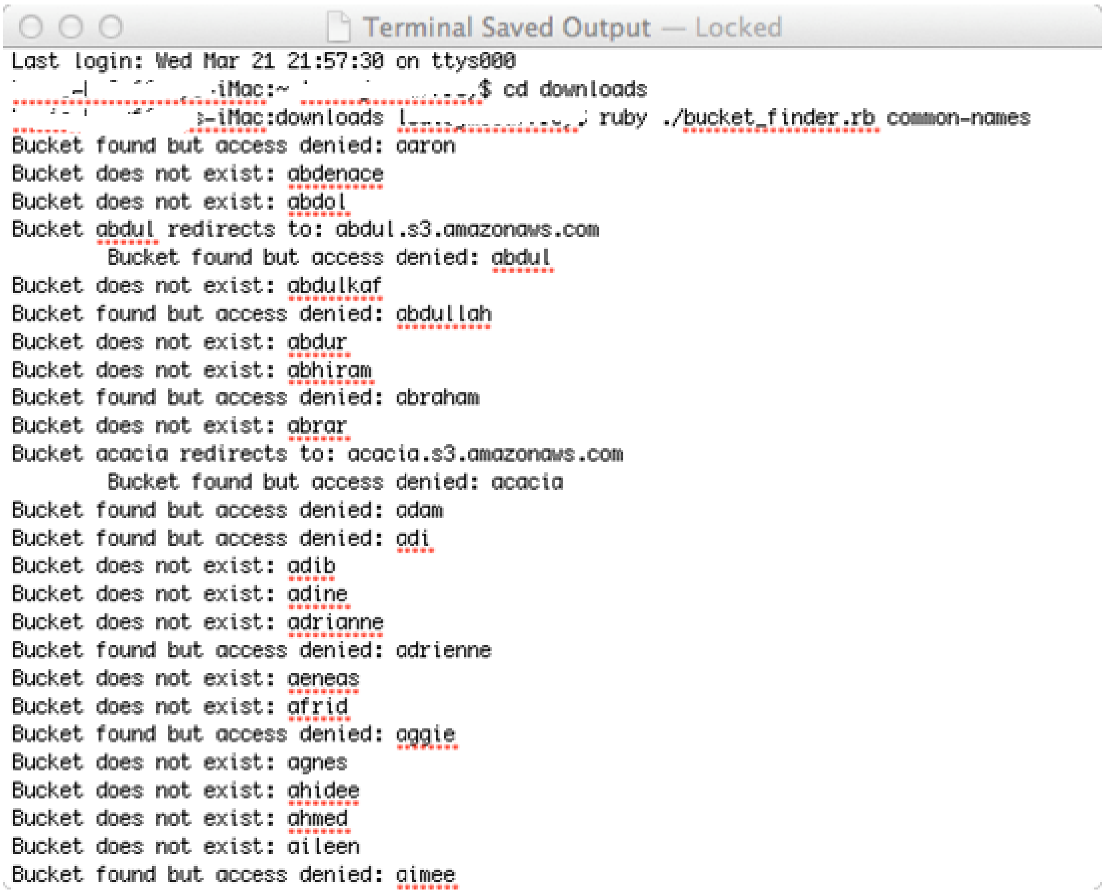
(Figure 6)

Once the word list was placed within the correct folder, alongside the ruby written ‘Bucket Finder’ tool, a terminal window was opened and the following command inputted:

```
$ ruby ./bucket_finder.rb common-names
```

This command was issued so as the bucket finder tool could then search through the Amazon S3 database in an attempt to match real buckets to the names contained in the word list. The bucket finder tool took roughly 50 minutes to scan through the word list and display whether or not the buckets, and the files contained in them, existed or not.

Figure 7 below shows the starting point of the experiment, where the command to begin the search was given, and the bucket finder tool began to scan through the word list.



```
Last login: Wed Mar 21 21:57:30 on ttys000
[redacted]-iMac:~ [redacted]$ cd downloads
[redacted]-iMac:downloads [redacted] ruby ./bucket_finder.rb common-names
Bucket found but access denied: aaron
Bucket does not exist: abdenace
Bucket does not exist: abdol
Bucket abdul redirects to: abdul.s3.amazonaws.com
        Bucket found but access denied: abdul
Bucket does not exist: abdulkaf
Bucket found but access denied: abdullah
Bucket does not exist: abdur
Bucket does not exist: abhiram
Bucket found but access denied: abraham
Bucket does not exist: abrar
Bucket acacia redirects to: acacia.s3.amazonaws.com
        Bucket found but access denied: acacia
Bucket found but access denied: adam
Bucket found but access denied: adi
Bucket does not exist: adib
Bucket does not exist: adine
Bucket does not exist: adrianne
Bucket found but access denied: adrienne
Bucket does not exist: aeneas
Bucket does not exist: afrid
Bucket found but access denied: aggie
Bucket does not exist: agnes
Bucket does not exist: ahidee
Bucket does not exist: ahmed
Bucket does not exist: aileen
Bucket found but access denied: aimee
```

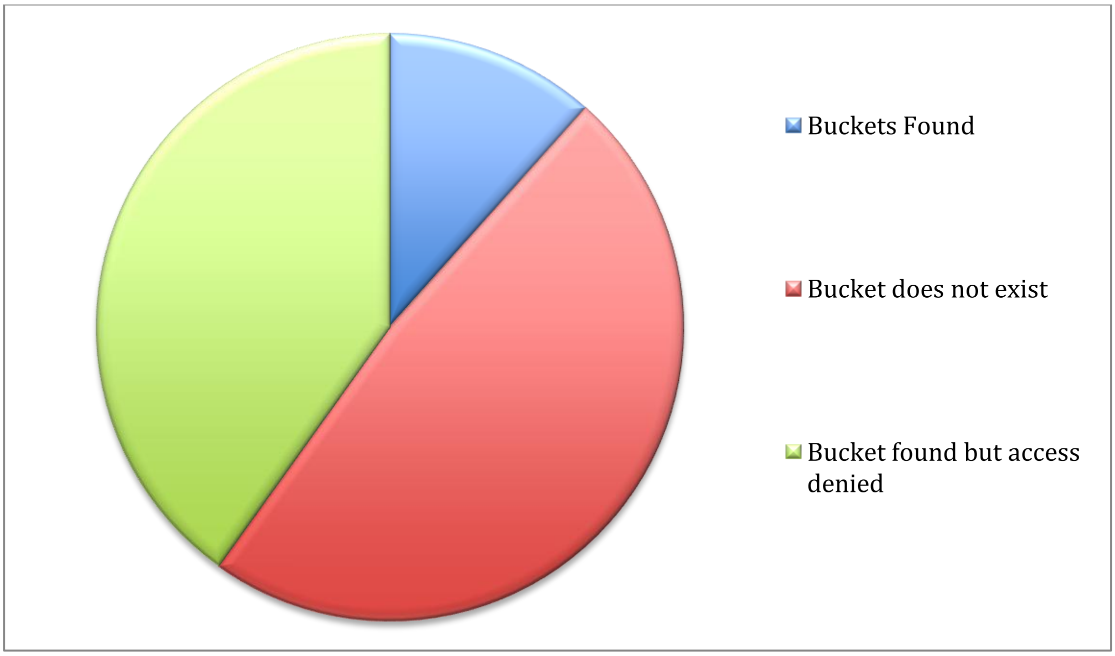
(Figure 7)

A shown in figure 2, the bucket finder tool attempts to find the buckets and the status of security within each bucket. There were various different responses from the database. If the bucket name did not exist, the bucket finder tool simply responds with the message “Bucket does not exist”, however if the bucket is found the tool will reply with the message, “bucket found”.

If the buckets are private and therefore access to the bucket and the files within it are denied, the bucket finder tool will also discover this and report this back to the user.

When buckets are found to exist and are also publically accessible, the tool then displays all the files that are found to be contained within those public buckets. However the access rights of the individual files are also displayed, but crucial information such as file names and file types are all still visible regardless of private status.

4.1.2 Buckets within Amazon S3



(Figure 8)

Figure 8 above is a visual representation of the results, which were gathered during this first experimentation stage. The bucket finder tool matched 116 buckets to the list of names within the word list. This means that 12% of the list of common names, which was searched, resulted in a bucket, which was publically accessible, being found. This also means that of these 116 buckets, hundreds of files were accessible, regardless of sensitivity or confidentiality.

It could be said that with these buckets being public buckets, the user has allowed these files to be accessed publically, however as the following section of this chapter highlights, some of the files which were found could be classed as sensitive information, therefore it could be true that users are unaware that their buckets, and also files, are actually accessible to anyone with the means of searching for them within the Amazon S3 database of buckets.

The results of the experiment also showed that 401, 40% of the total number of names searched actually resulted in a bucket being found however access was denied. This shows that users have ensured that they set the security parameters of their bucket to prevent unauthorised access. This shows that 52% of the common names contained within the word list used resulted in a bucket being found within the Amazon S3 cloud platform.

The largest proportion of results showed that no bucket existed for those particular names that were searched. Therefore 483 out of the 943 common names that were used within the wordlist did not have a corresponding bucket.

4.1.3 Files found within Amazon S3

Figure 9 shown below, highlights the number of files, which were found throughout this experiment into Amazon S3 global buckets. Each of these files were made publically accessible as a results of no security features protecting them. Whether these files were meant to be made public is unclear however throughout this experiment into these amazon S3 buckets, files and in particular photographic material has been found which may indeed have been confidential, however as a result of having no form of security within the cloud service to protect them, this experiment was able to access them.

Status of Files	Number of Files
Private	2,901
Public	1,658
Total files	4,559

(Figure 9)

In total 4,559 files were found as a result of this experiment. However despite this large number of files being found, 1,658 of these files were actually accessible. This meant that these files, regardless of content, were available to view and download. Users may therefore not be fully aware that their files are easily read by person(s) with the ability to source their buckets. It is important to note that 2,901 of the total files found were in fact private and securely protected against unauthorised access. Attempting to access private files will be discussed further in the following sections of this paper.

The nature of the files found due to this research varied in file type, size and sensitivity. Figure 5 which is displayed below offers more detail into the individual files found as a result of this research.

One interesting thing of note is that although 2,901 files were found to be private files, the file names and file extensions were still clearly visible; therefore information can still be gained about the private files contained within these amazon S3 buckets. This is an important aspect of the security which may require further attention by the service company, Amazon, as this allows hackers the means to see what files are contained in which buckets by a similar experimental process this paper has undertaken. A various number of hacking methods could be used in order to gain unauthorised access to these private files, with the knowledge of file name and file type.

None of the files which were found as a result of this experiment were downloaded, however a sample of the files were viewed to find out the sensitivity of the content which these public buckets contained. The varying nature of the files found shows that users of this cloud service use it to store all different types of data. This could highlight one fault with bucket policy’s, which will be described in greater detail to come, however this research has shown that users may have public and private files within buckets that are public in accessibility.

File Types	File Extensions	Number of files
IMAGES	JPG/PNG/GIF	1,600
WEB	CSS/HTML	97
VIDEO AND MUSIC FILES	AVI/MP3/MP4/FLV/MOV	292
DOCUMENTS	TXT/PDF/DOC	70
ARCHIVE FILES	ZIP/GZ	557
OTHER		1,943
TOTAL		4,559

(Figure 10)

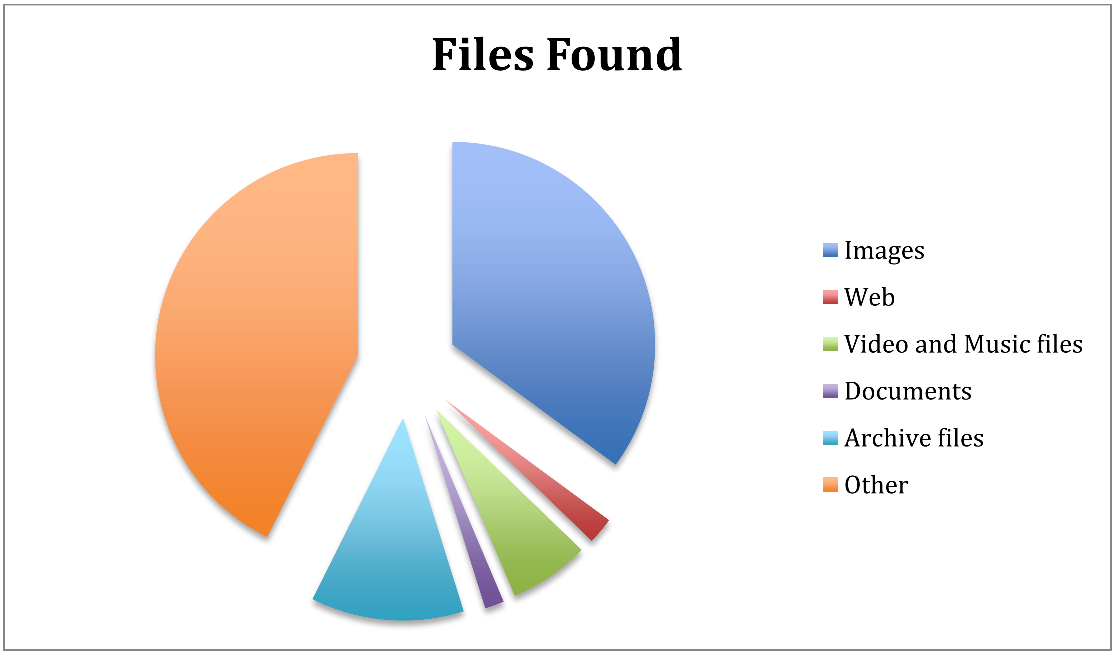
Figure 10 above tables the files that were found as a result of this experiment. As shown in the table the majority of the files found were image files. 1,600 image files in JPG, PNG and GIF formats were stored within these buckets, although some of these images were private. Of the image files which were viewed the majority of them were family pictures with children, these pictures may be public for a reason however some maybe be personal and confidential yet they were still accessible.

The music and video files which were found as a result of this research were mainly promotional videos for business or training videos for employees of companies; however this again highlights that the security of these files was non-existent, yet they could have displayed personal company information. The music files found collated to be a huge catalogue of music, which could be downloaded for free despite copyright laws. This yet again highlights the lack of security within the Amazon S3 cloud platform, or at least that users are not implementing sufficient security procedures to protect this amount of data.

The documents that were found produced some very interesting results. Of the selected documents that were viewed as part of this experiment, a large number of them contained personal and confidential information. Job application forms which contained personal information such as nation insurance numbers, and company documents detailing accounting information as well as other highly confidential data, were all found as a result of this search into public buckets.

One of the key findings of this research is that a high number of people put private files within publically accessible buckets, therefore meaning that unauthorised personnel could still gain access to key information contained within these buckets.

Figure 11 below shows a graphically representation of the results this experiment found into the files which are stored within these buckets. It is clear to see that the Amazon S3 cloud service is used by a large number of users to store sometimes highly personal image files, so as they may be shared at the users discretion. However as this research has found, it remains possible for unauthorised persons to access this material as there is insufficient security mechanisms I place to safe guard the material contained within this public buckets.



(Figure 11)

Image files equated for 35% of the overall number of files found through this research. Archive files, for example RAR, ZIP and GZ files were found to take up 12% of the overall number of files found. Video and music files also had a high percentage among these results with 6%.

4.2 Bucket Policy Access Control Results

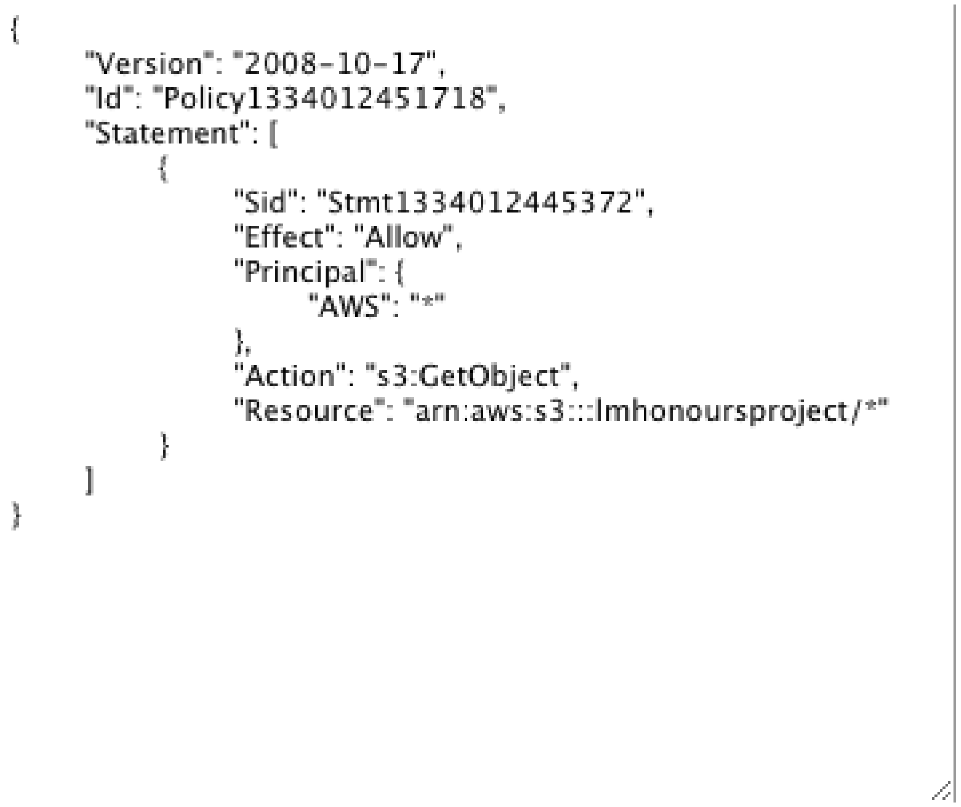
Bucket access control is the most important aspect of the security within this cloud service. As the results displayed within the previous sections details, the access to the buckets and files users have within Amazon S3 is of high importance and must be controlled accordingly.

The second part of the experimental process involved placing various test files within the test bucket. Firstly a set of test files including a txt document, a PDF document, and a TIFF image file were all placed within the test bucket ‘lmhonoursproject’.

In order to evaluate the bucket access policies within the Amazon S3 platform, a series of bucket policies were written then applied to the bucket. Amazon does not write bucket policies as standard, therefore the user must write their own bucket policy before applying that policy. Despite not writing the policy for users, amazon does provide a policy generator to help users create such access policies due to the programming language nature of the policies.

The bucket finder tool used in the previous experiment stage will again be used to test the access policies created for the test bucket.

Figure 12 below shows the first bucket policy which will be applied to the bucket for testing. It should allow everyone access to the bucket and the files within it.



```
{
        "Version": "2008-10-17",
        "Id": "Policy1334012451718",
        "Statement": [
                {
                        "Sid": "Stmt1334012445372",
                        "Effect": "Allow",
                        "Principal": {
                                "AWS": "*"
                        },
                        "Action": "s3:GetObject",
                        "Resource": "arn:aws:s3:::lmhonoursproject/*"
                }
        ]
}
```

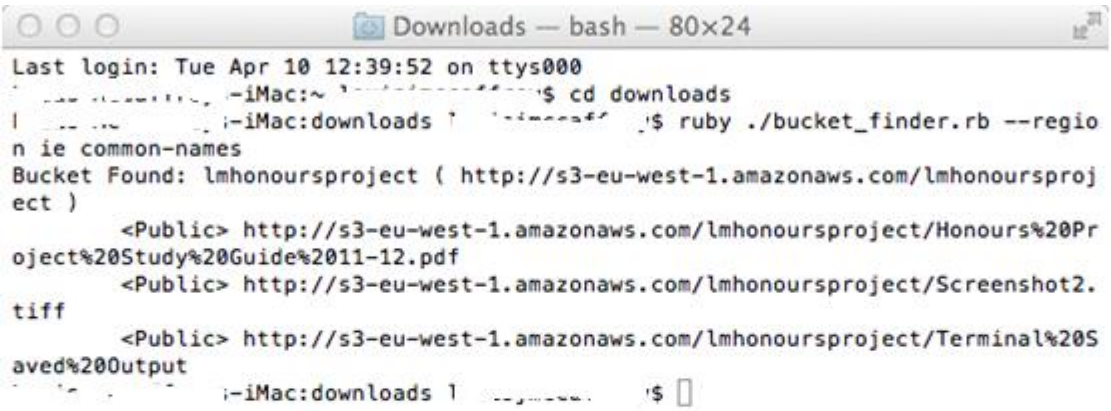
(Figure 12)

Once this policy had been created using the AWS policy generator, and applied to the test bucket, in this case ‘lmhonoursproject’, the bucket finder tool was then used to test the level of access, which could be gained. The following command was issued within the terminal window:

$ ruby ./bucket_finder.rb --region ie common-names

As the bucket finder tool requires a wordlist in order to function, the previous word list titled ‘common-names’ was edited to only include the name of the test bucket, ‘lmhonoursproject’.

As a result of this experiment the bucket finder tool found the test bucket, and was able to access it in order to list the files contained within it. Figure 13 below shows the results of the bucket finder tool experiment.



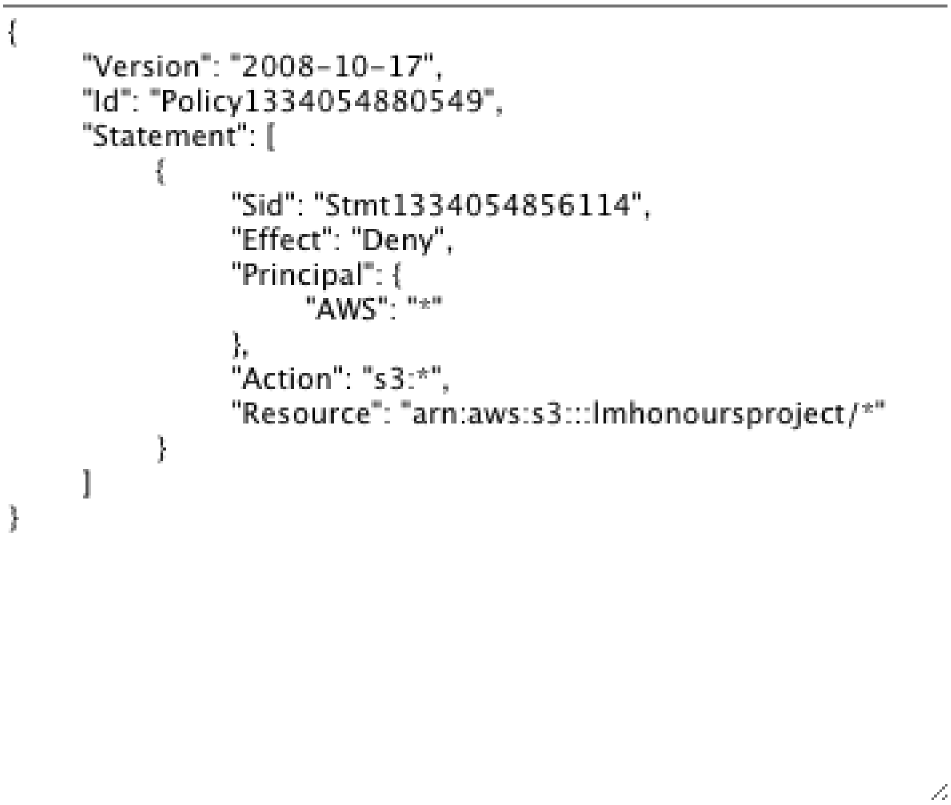
```
Last login: Tue Apr 10 12:39:52 on ttys000
[redacted]-iMac:~ [redacted]$ cd downloads
[redacted]-iMac:downloads [redacted]$ ruby ./bucket_finder.rb --regio
n ie common-names
Bucket Found: lmhonoursproject ( http://s3-eu-west-1.amazonaws.com/lmhonoursproj
ect )
        <Public> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Honours%20Pr
oject%20Study%20Guide%2011-12.pdf
        <Public> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Screenshot2.
tiff
        <Public> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Terminal%20S
aved%20Output
[redacted]-iMac:downloads [redacted]$ ▯
```

(Figure 13)

Conclusion: This Amazon S3 bucket policy allowed access to anyone and made the bucket completely public.

The second part of this experiment was to write a bucket policy that would restrict access so as only the administrator of the bucket could access the contents, therefore making the bucket completely private.

In order to begin this phase of the experiment another policy had to be written and applied. Figure 14 below shows the policy that was written in order to restrict access to the test bucket.



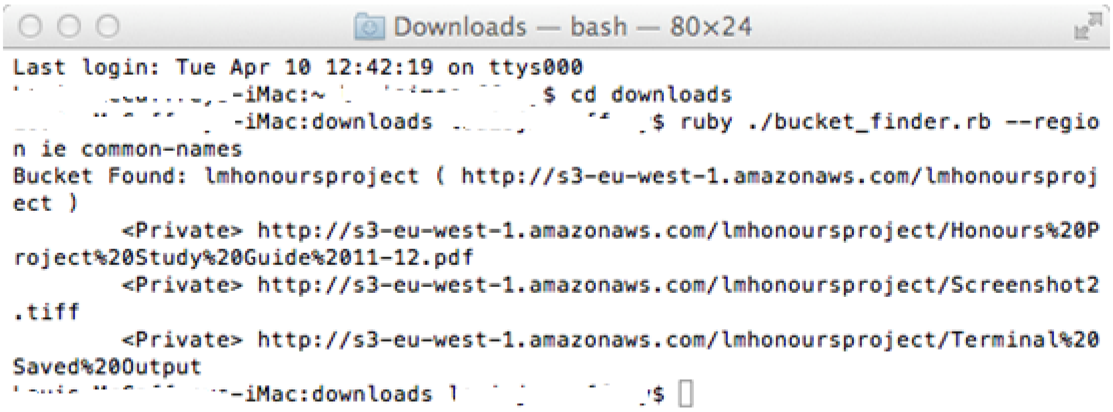
```
{
	"Version": "2008-10-17",
	"Id": "Policy1334054880549",
	"Statement": [
		{
			"Sid": "Stmt1334054856114",
			"Effect": "Deny",
			"Principal": {
				"AWS": "*"
			},
			"Action": "s3:*",
			"Resource": "arn:aws:s3:::lmhonoursproject/*"
		}
	]
}
```

(Figure 14)

Once this policy had been created using the AWS policy generator, and applied to the test bucket, again in this case ‘lmhonoursproject’, the bucket finder tool was then used to test the level of access, which could be gained. The previous command was again issued within the terminal window:

```
$ ruby ./bucket_finder.rb --region ie common-names
```

The bucket finder tool searched for the test bucket name contained in the word list, and correctly found the bucket. However instead of the bucket and files being public they were shown to be private, as shown in Figure 15 below.



```
Last login: Tue Apr 10 12:42:19 on ttys000
[redacted]-iMac:~ [redacted]$ cd downloads
[redacted]-iMac:downloads [redacted]$ ruby ./bucket_finder.rb --regio
n ie common-names
Bucket Found: lmhonoursproject ( http://s3-eu-west-1.amazonaws.com/lmhonoursproj
ect )
        <Private> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Honours%20P
roject%20Study%20Guide%2011-12.pdf
        <Private> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Screenshot2
.tiff
        <Private> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Terminal%20
Saved%20Output
[redacted]-iMac:downloads [redacted]$ ▯
```

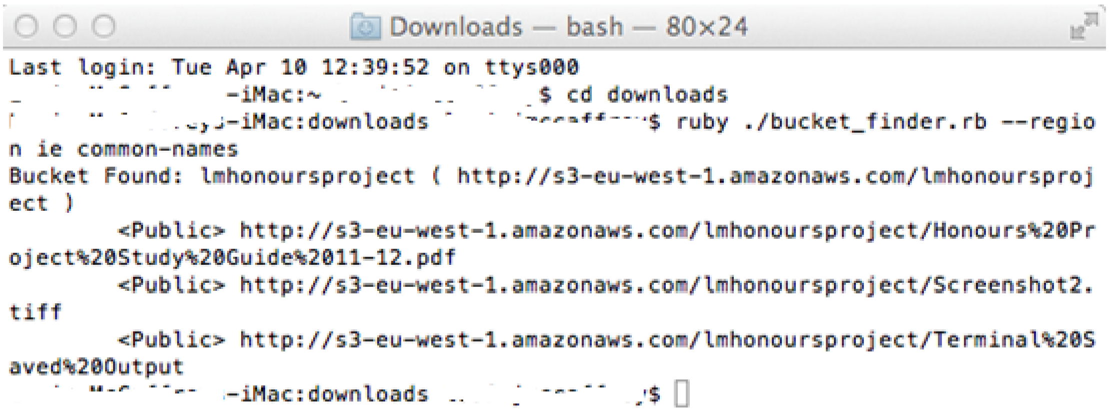
(Figure 15)

Conclusion: This bucket policy to deny access to any unauthorised user correctly prevented the bucket finder tool accessing the files within the bucket. Therefore the mechanism of bucket policies efficiently either granted permission of denied it based on the nature of the policy.

It can therefore be said that the results of this experimental process show that the Bucket policy security mechanism within Amazon S3 does in fact protect the data contained within the buckets.

4.3 Query String Authentication Results

The results from the previous stage of the experiment have shown that each test file within the test buckets also appeared to have a query sting authenticated URL attached to those files. Therefore a simple experiment was conducted to test this authentication mechanism as well as the accessibility of the files in general.



```
Last login: Tue Apr 10 12:39:52 on ttys000
[redacted]-iMac:~ [redacted]$ cd downloads
[redacted]-iMac:downloads [redacted]$ ruby ./bucket_finder.rb --regio
n ie common-names
Bucket Found: lmhonoursproject ( http://s3-eu-west-1.amazonaws.com/lmhonoursproj
ect )
        <Public> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Honours%20Pr
oject%20Study%20Guide%2011-12.pdf
        <Public> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Screenshot2.
tiff
        <Public> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Terminal%20S
aved%20Output
[redacted]-iMac:downloads [redacted]$ ▯
```

(Figure 16)

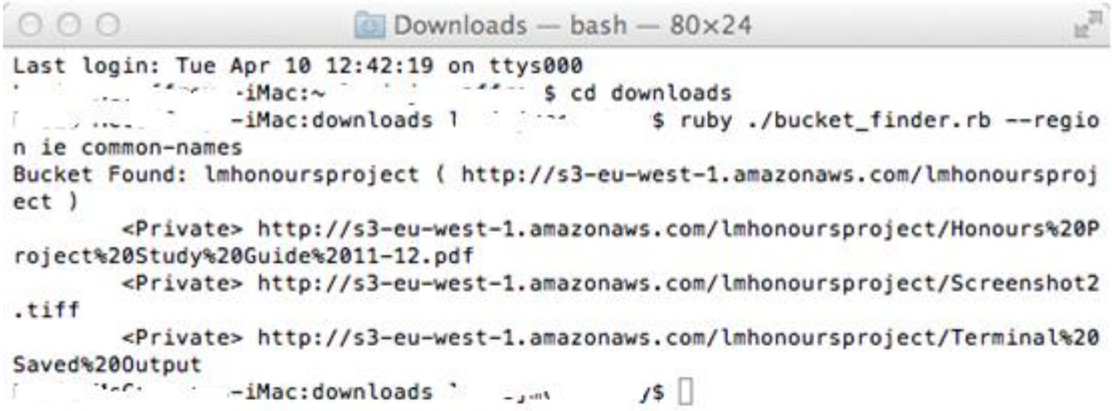
Figure 16 shows that each file listed within the test bucket had a corresponding URL which links to that file within the Amazon S3 system. These links also encompass the Query String Authentication security mechanism to grant or deny access.

This phase of the experiment required each URL to be copied into an Internet Browser. With the bucket policy granting access to the files, query string authenticated the URLs so as they could be viewed within the browser window.

Conclusion: Query String authentication granted access to the files contained within the test bucket as the bucket policy made the files public. Therefore authenticating the URL of the files allowed for access to those individual files stored within the bucket.

Despite the Query string Authentication allowing access to the files found within the test bucket with the URL of each file, another test had to be implemented to discover what would happen if the files were in fact private files. Would the query string authenticated URLs still allow access to the files within the bucket?

Again using the findings from the previous experimental phase, a test was carried out to assess the access of the URLs of the test files.



```
Last login: Tue Apr 10 12:42:19 on ttys000
[redacted]-iMac:~[redacted] $ cd downloads
[redacted]-iMac:downloads [redacted] $ ruby ./bucket_finder.rb --regio
n ie common-names
Bucket Found: lmhonoursproject ( http://s3-eu-west-1.amazonaws.com/lmhonoursproj
ect )
        <Private> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Honours%20P
roject%20Study%20Guide%2011-12.pdf
        <Private> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Screenshot2
.tiff
        <Private> http://s3-eu-west-1.amazonaws.com/lmhonoursproject/Terminal%20
Saved%20Output
[redacted]-iMac:downloads [redacted]/$ ▯
```

(Figure 17)

Figure 17 above shows the URL's of the test files, which are private files due to the bucket policy previously used within the experiment. Once again these same URL links were copied into an Internet browser, however this time these links gave the following message;

"AccessDeniedAccess Denied38E059155ED2C7EFY1Qh4C2hEhTO9NQVuDIuWXtbZbv7kTgTEM9zrZv3GgholbHx9OKIrDaNa48oSKDY"

Conclusion: The query string authenticated URL denied access to the files within the test bucket in accordance with the bucket policy written to the test bucket. This proves that the Query String Authentication security mechanism can allow access to a files, using a URL, however only when the bucket policy allows.

5 Discussion and Conclusions

This chapter will detail the final conclusions of this experimental project based on the findings found within chapter 4. The following sections will offer a brief summary of the project as well as a discussion based on the results that were gathered throughout the experimental phase. The research question, which was highlighted within chapter 1, will be discussed and answered. Possible future development of this project will be discussed also.

5.1 Project Summary

Cloud computing is becoming increasingly popular both to individual users and business users. With a greater number of well-known companies adopting/offering cloud computing services, the question of data security has been widely debated. One of the largest cloud computing services in operation today is Amazon's S3 cloud storage service. The whole nature of storing personal information out with the user's physical devices causes many potential users to hesitate in embracing the technology. Therefore an investigation into the security mechanisms within, as previously stated, one of the most popular cloud storage services, Amazon S3, was required to determine if these current security measures were effective and reliable. This investigation led to the following research question:

Are the current security mechanisms', including query string authentication and bucket polices, within the Amazon S3 cloud-computing platform, effective in protecting the data and files of its users?

In order to answer this research question an investigation into cloud computing security was undertaken. Further investigations were conducted into the various common security mechanisms used to protect data within cloud services. After reviewing the findings of these investigations a series of experiments were conducted to evaluate the security features within the Amazon S3 cloud service. These experiments focused on access data held within the cloud. The results of the experimentation phase of the project, detailed in Chapter 4, helped analyses the way a typical cloud service works, as well as the ability/inability of unauthorised user to access that data held within the cloud.

5.2 Discussion of Results

The results retailed within chapter 4, show that access to the buckets and files stored within them, is not always as secure as it should be. The first experiment conducted into access of global Amazon S3 buckets showed that lots of personal and private information was available to unauthorised users, as a result of poor access precautions being implemented to protect this data. The use of the Bucket Finder tool was critical in searching through the Amazon bucket database in order to evaluate the level of security. The results of that particular phase of experimentation highlighted that many users name there storage buckets after things which are easy to guess for hackers, for example their own name, which was of course used within the wordlist of common names.

Gaining information about a storage bucket as a result of knowing just the name of the bucket highlights a weakness in security. As a result of searching through the database of buckets with the Bucket Finder tool matched against the constructed word list, it was found that of the 943 names contained within the word list, 517 of those names had a corresponding storage bucket.

Further investigation into the access levels of these buckets revealed that 116 of those buckets found, were public and therefore it was possible to see the files that were contained within those buckets. As a result it was possible to see the file names, files types and URLs of these files.

The next stage of the investigation was to analyse the files that were found to be contained within these public buckets. The experiment resulted in a total of 4,559 files being found, with 1,658 of these files being publically accessible. Analysing a proportion of these public files showed that the majority of these files were in fact image files. These images were varied in nature, however a large number were family photos including children. There are of course justified reasons for these files being made public however it remains possible that these images could be publically accessible without the owner realising the opportunity for unauthorised persons to access this material. Further research into other public files found within public buckets, unveiled important and highly confidential information contained within job applications forms and also business records, which include company accounts information. The nature of this information is private however these files were not protected or made completely private.

Another interesting finding of the experiment was that private files can be stored within public buckets, however the file names, and file extensions of these private files are still visible. Therefore there is potential for a hacker to gain unauthorised access to these files as a result of knowing the file location, name and type.

This first stage of experiment into Amazon S3 cloud storage security has shown that with security measures in place, the data is efficiently protected; however there are still various aspects of the security that could be further tightened. However despite focusing one the security measures available to the user, it is important to highlight that users must take responsibility for their data and protect it themselves with the aid of the mechanisms available to them.

The second phase of the experimentation stage was to construct two contrasting bucket access policies in order to evaluate the Bucket policy security mechanism. Bucket policies allow users to write an access policy to the bucket containing the files they wish to protect; therefore restricting access to the bucket also restricts access to all the files housed within it.

The first step in this experiment was to create a bucket policy, which would allow access to all the files within the test bucket. Figure 12 shows the exact policy that was written for the experiment. This policy was then applied to the bucket. Then next stage was to again use the bucket finder tool to test the access of the files. As expected the bucket finder tool searched for the test bucket within the database and returned information, Figure 13, which indicated that the bucket was in fact publically accessible, and so to where the files within the bucket. This experiment proved that the bucket policy mechanism worked and allowed access to the files as a result.

The second step of this experiment into bucket policy was to write a contrasting policy that would restrict access to the bucket and files so that only the owner of the bucket would be able to gain access. Figure 14 shows the policy that was written and applied to the test bucket. Again the bucket finder tool was used to test the effectiveness of this bucket policy mechanism. This experiment resulted in the bucket and files being private and therefore inaccessible, however crucially important information regarding these now private files was still displayed, as shown in Figure 15.

This experiment into Bucket policies has shown that the mechanism does effectively protect the information contained within the bucket; however one possible weakness is that information regarding the private files is still accessible. An overall conclusion into bucket policies can be drawn as a result; the mechanism of bucket access policies can be used in order to restrict or grant access to files stored within Amazon S3 buckets.

The final phase of the experimental process was to conduct an evaluation into the query string authentication mechanism used to grant or deny access to files. The experiments previously conducted, highlighted that each file had a corresponding URL. These URLs use query string authentication as a method of protecting the files against unauthorised access.

A simple experiment was conducted whereby the URL’s of each test file found when the bucket policy had made access to the files public were copied into an Internet Browser in order to gain access to the files. The results of this first stage of experiment showed that the query string authentication mechanism allowed access to the files as a result of the bucket policy granting overall access to the bucket and its contents.

The second stage of experiment into query string authentication saw the previous experiment being repeated for the files once the bucket policy had changed to private. When copying the URLs of each file into an Internet browser, instead of the pervious result allowing access to the files, a message was displayed within the browser stating that access to the files was denied.

This experiment into query string authentication has shown that the bucket policy, which is also implemented within the bucket, has a direct impact on this mechanism. More complex query string authentication methods could be conducted with future development.

The findings of the whole experimentation process have allowed for further analysis and supplied enough evidence to answer the research question and as a result partially elevating fears of cloud storage security.

5.3 Project Limitations and Future Development

There are many other areas of cloud computing security that this project did not have the scope to investigate. The experiment involved within this paper only evaluates one particular cloud storage service Amazon S3; however future development could include investigations into other major cloud services that not only store the data but also stream the data to multiple devices.

With regards to Query String Authentication, this experimental project was limited to recording results in a live situation however further investigation of this security mechanism could take into account features like time limits which can be placed on the URLs of files.

Further development into bucket policies could be conducted to investigate more complex access policies associated to the buckets and files within them.

5.4 Conclusion

This project was developed in order to critically evaluate the effectiveness of security procedures/mechanisms within one of the most popular cloud storage platforms, Amazon S3. The analysis and results documented throughout chapters 4 and 5 provide various conclusions with reference to the research question as well as the project objectives. This analysis was possible as a result of the extensive literature review that was first carried out, and also the well planned experiment methodology.

The findings into cloud security this paper has detailed will be of particular interest to the millions of users, which entrust their personal and private data to this third party service. The finding will serve to alleviate some fears of the dangers cloud data storage brings. Therefore not only will this research be of interest to current users of cloud technology but also to persons yet to embrace it. Many businesses are looking towards cloud-based solutions for their data storage, so the scope of interest into the finding of this paper will be far reaching.

It is clear from conducting this evaluation of Amazon S3's security mechanisms that cloud computing and in particular cloud storage will continue to grow and gain in popularity. The security fears expressed within the literature review highlight the public perception of cloud storage, which individuals as well as business users, must change if this technology is to become a universal standard.

Through the undertaking of this project, the experiments into security that were extensive and appropriate, and lastly the critical analysis of the results these experiments returned, an overall conclusion can be reached that the security procedures and mechanisms in place within the Amazon S3 service, effectively and efficiently protect the data users place within it.

6 References

Aljabre, A. 2012, "Cloud Computing for Increased Business Value", *International Journal of Business and Social Science,* vol. 3, no. 1.

, *Amazon Simple Storage Service (Amazon S3)* . Available: http://aws.amazon.com/s3/ [2011, 11/3/2011].

Anthes, G. 2010, "Security in the Cloud", *Association for Computing Machinery.Communications of the ACM,* vol. 53, no. 11, pp. 16.

Barnes, F., JD 2010, "Putting a lock on Cloud-Based Information", *Information Management Journal,* vol. 44, no. 4, pp. 26.

Blandford, R. 2011, "Information security in the cloud", *Network Security,* vol. 2011, no. 4, pp. 15.

Blumenthal, M. 2011, "Is Security Lost in the Clouds? (*)", *Communications & Strategies,* , no. 81, pp. 69.

Bowers, K.D., Juels, A. & Oprea, A. 2009, "HAIL: A high-availability and integrity layer for cloud storage", *Proceedings of the 16th ACM conference on Computer and communications security*ACM, , pp. 187.

Bowers, L. 2011, "Cloud Computing Efficiency", *Applied Clinical Trials,* vol. 20, no. 7, pp. 45.

Bradshaw, S., Millard, C. & Walden, I. 2011, "Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services", *International Journal of Law and Information Technology,* vol. 19, no. 3, pp. 187-223.

Cachin, C. & Schunter, M. 2011, "A cloud you can trust", *IEEE Spectrum,* vol. 48, no. 12, pp. 28.

Castelluccio, M. 2010, "A Pocketful of Clouds", *Strategic Finance,* vol. 92, no. 6, pp. 59.

"Cloud Providers Aren't Much Concerned with Security", 2011, *Information Management Journal,* vol. 45, no. 4, pp. 7.

"Cloud Security Alliance and IEEE Join Forces to Identify Cloud Security Standards Requirements For IT Practitioners", 2010, *Business Wire,* .

, *Cloud Security Alliance* . Available: https://cloudsecurityalliance.org/ [2011, 11/3/2011].

Das, S., Du, A., Gopal, R. & Ramesh, R. 2011, "Risk Management and Optimal Pricing in Online Storage Grids", *Information Systems Research,* vol. 22, no. 4, pp. 756.

"Document Exchange and Collaboration Between Amazon S3, Google and Microsoft SharePoint", 2010, *International Journal of Micrographics & Optical Technology,* vol. 28, no. 3, pp. 3.

"Federal Govt. Still Wary of the Cloud", 2010, *Information Management Journal,* vol. 44, no. 4, pp. 15.

Gable,J.,CRM, FAI 2011, "Lifting the Fog on Cloud Computing", *Information Management Journal,* vol. 45, no. 6, pp. 46.

Gold, S. 2010, "Protecting the cloud: attack vectors and other exploits", *Network Security,* vol. 2010, no. 12, pp. 10.

Han, Y. 2011, "Cloud Computing: Case Studies and Total Costs of Ownership", *Information Technology and Libraries,* vol. 30, no. 4, pp. 198.

Harnik, D., Kolodner, E.K., Ronen, S., Satran, J., Shulman-Peleg, A. & Tal, S. "Secure Access Mechanism for Cloud Storage", .

Hocking, M. 2011, "Thin client security in the cloud", *Network Security,* vol. 2011, no. 6, pp. 17.

Hofmann, P. & Woods, D. 2010, "Cloud Computing: The Limits of Public Clouds for Business Applications", *IEEE Internet Computing,* vol. 14, no. 6, pp. 90.

Kabay, M.E., Miora, M., Cissp-Issmp & Fbci 2011, "Using cloud computing and storage for business continuity", *Network World (Online),* .

Khan, K. & Malluhi, Q. 2010, "Establishing Trust in Cloud Computing", *IT Professional Magazine,* vol. 12, no. 5, pp. 20.

Lakshminarayanan, S. 2010, "Interoperable Security Standards for Web Services", *IT Professional Magazine,* vol. 12, no. 5, pp. 42.

Maitner,R., Jr,CGFM, PMP 2011, "Moving to the Cloud: Is Federal Financial Management Fair Game?", *The Journal of Government Financial Management,* vol. 60, no. 3, pp. 52.

Mansfield-Devine, S. 2008, "Danger in the clouds", *Network Security,* vol. 2008, no. 12, pp. 9.

Morrell, R. & Chandrashekar, A. 2011, "Cloud computing: new challenges and opportunities", *Network Security,* vol. 2011, no. 10, pp. 18.

Popa, R.A., Lorch, J.R., Molnar, D., Wang, H.J. & Zhuang, L. 2010, "Enabling security in cloud storage SLAs with CloudProof", *Microsoft TechReport MSR-TR-2010,* vol. 46.

Ren, K., Wang, C. & Wang, Q. 2012, "Security Challenges for the Public Cloud", *IEEE Internet Computing,* vol. 16, no. 1, pp. 69.

"Research and Markets: Business in the Cloud: What Every Business Needs to Know About Cloud Computing", 2011, *Business Wire,* .

Rose, C. 2011, "A Break In The Cloud? The Reality Of Cloud Computing", *International Journal of Management and Information Systems,* vol. 15, no. 4, pp. 59.

Sehgal, N., Sohoni, S., Xiong, Y., Fritz, D., Mulia, W. & Acken, J. 2011, "A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing", *IETE Technical Review,* vol. 28, no. 4, pp. 279.

Srinivasan, M. 2010, "Cloud Security for Small Businesses", *Allied Academies International Conference.Academy of Information and Management Sciences.Proceedings,* vol. 14, no. 1, pp. 72.

Stoller, J. 2011, "Moving up from shrink wrap: When is it time to make the leap?", *CMA Magazine,* vol. 85, no. 3, pp. 32.

Switzer, D. & Rajachandrasekar, R. "On Clouds, Cloud Security and Dependability", .

Vogels, W. 2009, "Eventually Consistent", *Association for Computing Machinery.Communications of the ACM,* vol. 52, no. 1, pp. 40.

Walters, R. 2010, "Managing privileged user activity in the datacentre", *Network Security,* vol. 2010, no. 11, pp. 6.

Wang, C., Wang, Q., Ren, K. & Lou, W. 2010, "Privacy-preserving public auditing for data storage security in cloud computing", *INFOCOM, 2010 Proceedings IEEE*IEEE, , pp. 1.

Wang, C., Ren, K., Lou, W. & Li, J. 2010, "Toward Publicly Auditable Secure Cloud Data Storage Services", *IEEE Network,* vol. 24, no. 4, pp. 5.

Wang, W., Rashid, A. & Chuang, H. 2011, "Toward the Trend of Cloud Computing", *Journal of Electronic Commerce Research,* vol. 12, no. 4, pp. 238.

Zarandioon, S., Yao, D. & Ganapathy, V. "K2C: Cryptographic Cloud Storage With Lazy Revocation and Anonymous Access", .

Zhou, L., Varadharajan, V. & Hitchens, M. 2011, "Enforcing Role-Based Access Control for Secure Data Storage in the Cloud", *The Computer Journal,* vol. 54, no. 10, pp. 1675.

7 Bibliography

, *Amazon Simple Storage Service (Amazon S3)* . Available: http://aws.amazon.com/s3/ [2011, 11/3/2011].

"Cloud Storage Security Demonstrated With Bold Challenge", 2010, *International Journal of Micrographics & Optical Technology,* vol. 28, no. 3, pp. 8.

, *Cloud Security Alliance* . Available: https://cloudsecurityalliance.org/ [2011, 11/3/2011].

Hocking, M. 2011, "Thin client security in the cloud", *Network Security,* vol. 2011, no. 6, pp. 17.

Katzan, H.,Jr 2010, "On The Privacy Of Cloud Computing", *International Journal of Management and Information Systems,* vol. 14, no. 2, pp. 1.

Mulazzani, M., Schrittwieser, S., Leithner, M., Huber, M. & Weippl, E. "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space", .

Ruwei, H., Xiaolin, G., Si, Y. & Wei, Z. 2011, "Study of privacy-preserving framework for cloud storage", *Computer Science and Information Systems,* , no. 00, pp. 29-29.

Singh, S. 2011, "Computing Without Processors", *Association for Computing Machinery.Communications of the ACM,* vol. 54, no. 8, pp. 46.

Taylor, M., Haggerty, J., Gresty, D. & Lamb, D. 2011, "Forensic investigation of cloud computing systems", *Network Security,* vol. 2011, no. 3, pp. 4.

Thomas, P.Y. 2011, "Cloud computing", *The Electronic Library,* vol. 29, no. 2, pp. 214.

Valafar, M. & Butler, K. "Poster: Secure Provenance for Cloud Storage", .

Walsh, P. 2009, "The brightening future of cloud security", *Network Security,* vol. 2009, no. 10, pp. 7.