ANALYSIS OF SECURITY VULNERABILITY IN DROPBOX CLOUD DATA EXCHANGE AND STORAGE

BY

SAMUEL KINUTHIA NDURA
I132/0868/2013

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT TO THE SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS FOR THE AWARD OF BACHELORS DEGREE IN COMPUTER SECURITY AND FORENSICS AT JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

DECEMBER 2016

DECLARATION

I declare that this research project is my original work and has not been presented for an award of a diploma or conferment of a degree in any other university or institution.

Signature Date

…… ……

SAMUEL KINUTHIA NDURA

REG. No. I132/0868/2013

This research project has been submitted with my approval as the university supervisor

Signature Date

…… ……

MR. JOSHUA AGOLA

SUPERVISOR

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEDICATION

This research project is dedicated to my parents, Mr. James Ndura and Mrs. Lucy Ndura whose love, sacrifice and commitment towards giving each and every one of us education remains unrivalled.

ACKNOWLEDGEMENT

First of all I would like to thank the Almighty God for giving me this opportunity and the far he has brought me. I would like to thank Him for His protection during the whole university period, His protection and care.

My other appreciation goes to the School of Informatics and Innovative Systematics for the skills and knowledge they have offered me for a period of four years. Thank you so much for helping me in all ways pertaining to my field of study. Thanks to my university based supervisor, Mr. Joshua Agola, for taking his time to guide me through my research project. His guidance and recommendation on how to go about my research project problems. Receive my sincere thanks.

Sincere thanks to my parents, Mr. James Ndura and Mrs. Lucy Ndura for their financial and moral support. Their guidance during the period and during the preparation of this research project was so helpful to me. My siblings Eunice, Zachariah, Sarah, Elizabeth and Hope who have been great inspiration to me in my pursuit of academic endeavors, thank you so much.

My friends with special thanks to Oliver Nyaswenta and Mungai Reuben, who helped me all through my university academic life and more so in the research process correcting me and offering support. Thank you so much.

Thank you all and the Almighty God bless you.

ABSTRACT

The world is now storing private personal and business data in the cloud. Dropbox cloud storage provides an ideal platform where particular users can store their data in the cloud and later access it via the internet from any geographical position. In order to access this data, providers such as photo sharing services or general purpose storage services are expected to be accessible not only by the browsers but also by apps that leverage that data to enhance user experience. In an effort to ease he development lifecycle and encourage an ecosystem of reliable solutions, cloud services often provide a framework that apps can utilize. From a security perspective however, the frameworks themselves provide an extremely attractive attack surface since the vulnerability of the framework could potentially affect numerous applications that use it. This paper, is going to analyze the security vulnerabilities data is subjected to in Dropbox cloud storage during data transit and data storage. Using previously reported cases and previous works done by other scholars the research is going to outline the various attack techniques utilized by hackers to access data in the cloud. The research project will finally finish my research project by recommending various ways Dropbox cloud storage users can ensure security of their data

TABLE OF CONTENTS

List of Figures

CHAPTER ONE
INTRODUCTION

1.1 Introduction of Cloud Computing

Personal cloud storage services are gaining popularity. With a rush of providers to enter the market and an increasing offer of cheap storage space, it is to be expected that cloud storage will soon generate a high amount of Internet traffic. Very little is known about the architecture and the performance of such systems, and the workload they have to face. This understanding is essential for designing efficient cloud storage systems and predicting their impact on the network (Marinescu, D. 2013).

Cloud computing was coined for what happens when applications and services are moved into the internet "cloud." Cloud computing is not something that suddenly appeared overnight; in some form it may trace back to a time when computer systems remotely time-shared computing resources and applications. It refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications.

Cloud computing can be used easily in one's personal life as well as in one's business life. It's highly likely that you already use at least one, if not many, cloud computing services. Additionally, as you explore the services we describe here, you may find that some of them may make your life easier, or help you in promoting, managing, or operating your business. That's what cloud computing is for. But before you decide to start using these services, make sure you read the rest of this site (Marinescu, D. 2013).

1.1.1 Uses of cloud Computing

i Hosting services

This has been made so popular by Google Docs which is a function brought by Google used to store and edit ones document online. This feature enables the documents to be accessible from anywhere and goes to a further step whereby you can share the documents and collaborate with them. It also allows multiple users to work on the document simultaneously (Rountree & Castrillo, 2014).

ii Backup services

Most people have their own ways of storing their information and documents. The most common one is whereby you store the documents and files on a personal computer. However the problem with personal computer (storage) is that there has been a big problem where data on one's computer is stolen destroyed or lost through damaged storage devices. Cloud computing can be used for backup services where your data is stored in data servers spread out around the world (Rountree & Castrillo, 2014).

iii E-Mail

This is one of the biggest cloud computing services which entail storage of web based emails. Using a cloud computing e-mail solution allows the mechanics of hosting an e-mail server and maintaining it to be taken out of the hands of the users. This also enables a person to be in a position to access all his e-mails from anywhere (Rountree & Castrillo, 2014).

iv Social Networking

This is the most famous use of cloud computing. However, it does not appear as such too many people. Social networking sites such as Facebook, LinkedIn, MySpace, Twitter etc. utilize cloud computing services. The data uploaded in social sites is directly stored in the cloud drives. This entails all information including personal profile details. This enables the person to be in a position to access their profile details from basically anywhere by use of the internet (Rountree & Castrillo, 2014).

1.1.2 Types of Cloud Computing

There are various types of cloud computing based in the different types of services offered. These are divided into four main categories. It is divided on factors based on the cloud location, or on the service that the cloud is offering (Rountree & Castrillo, 2014).

i Public

Public cloud implies that the whole computing infrastructure is located on the premises of a cloud computing company that offers the cloud service. The location is different from the customer and the customer does not have any physical control over it.

ii Private

Private cloud computing means using a cloud infrastructure (network) solely by one customer/organization. It is not shared with others, yet it is remotely located. If the cloud is externally hosted the companies have an option of choosing an on-premise private cloud as well, which is more expensive, but they do have a physical control over the infrastructure.

iii Hybrid

Hybrid cloud computing is whereby a company uses both private and public clouds, depending on their purpose. For instance, public cloud can be used to interact with customers, while keeping their data secured through a private cloud.

iv Community cloud

This implies an infrastructure that is shared between organizations, usually with the shared data and data management concerns. For example, a community cloud can belong to a government of a single country. Community clouds can be located both on and off the premises.

Basing on the service the cloud computing is offering it is divided into

i Infrastructure as a Service (IaaS)
ii Platform as a Service (PaaS)
iii Software as a Service (SaaS)

Or Storage, Database, Information, Process, Application, Integration, Security, Management, Testing-as-a-service

Cloud computing is vastly taking form in the computing world with a number of companies trying their best to offer these services. Among these companies include Google, Microsoft, Citrix, Amazon, IBM, Salesforce etc. some of these companies offer free cloud services while others users have to pay and the storage capacity is offered depending on the amount paid for. Some of these free companies include Box, Dropbox, Drive, iCloud, Amazon etc. (Rountree & Castrillo, 2014).

From a security perspective, however, the frameworks themselves provide an extremely attractive attack surface since the vulnerability of the framework could potentially affect numerous applications that use it. In this paper I will be talking about Dropbox, its functionalities, security vulnerabilities and how these vulnerabilities can be fixed.

1.2 Dropbox Cloud Computing

The world is now storing private personal and business data in the cloud. Dropbox provides a platform where a particular user can store data in the cloud and later access it from any location via the internet. In order to access this data, providers such as photo sharing services or general purpose storage services, are expected to be accessible not only by the user, but also by apps that leverage that data to enhance the user experience. In an effort to ease the development lifecycle and encourage an ecosystem of reliant solutions, cloud services often provide a framework that apps can utilize (Winder, 2016).

The Dropbox native client is implemented mostly in Python, using third-party libraries such as librsync. The application is available for Microsoft Windows, Apple OS X and Linux. The basic object in the system is a chunk of data with size of up to 4MB. Files larger than that are split into several chunks, each treated as an independent object. Each chunk is identified by a SHA256 hash value, which is part of meta-data descriptions of files. Dropbox reduces the amount of exchanged data by using delta encoding when transmitting chunks. It also keeps locally in each device a database of meta-data information (updated via incremental updates) and compresses chunks before submitting them (Winder, 2016).

In addition, the client offers the user the ability to control the maximum download and upload speed. Two major components can be identified in the Dropbox architecture. These are: the control and the data storage servers.

The control is under direct control of Dropbox Inc., while Amazon Elastic Compute Cloud (EC2) and Simple Storage Service (S3) are used as storage servers. In both cases, subdomains of dropbox.com are used for identifying the different parts of the service offering a specific functionality (Winder, 2016).

1.3 Problem Statement

There have been cases previously where attackers access your Dropbox and use it to carry out their malicious activity. This has led to a widespread of users losing their data and information stored in the drive. The problem goes further to a point where the hackers can access data in your computer through Dropbox and store or install malicious codes into your computer.

The IBM X-Force Research Team developed a working proof of concept exploit, dubbed DroppedIn to test this vulnerability (Hay, 2015). This proof of concept allows the attacker to link a target app with the attacker's Dropbox account instead of the victim's without the victim's knowledge. According to Roee Hay, we created both local and remote (drive-by) end-to-end versions of the DroppedIn proof of concept attack. Both local and remote attacks fail if the Dropbox app is installed on the targeted device. In order to exploit the DroppedIn vulnerability, a couple of things need to happen (Hay, 2015)

1.4 Objectives

1.4.1 Main objectives

i To enhance security in Dropbox cloud computing by suggesting some of the measures that can be implemented by users

1.4.2 Specific objectives

i To analyze security vulnerability in Dropbox and some of the causes

ii To identify some of the attacks that have previously been carried out on Dropbox and how they can be stopped

iii Suggest some of the ways a user can ensure security of their data and information stored in Dropbox cloud

1.6 Research Questions

i How secure is the data stored in clouds

ii What are some of the security vulnerabilities present in cloud computing and what are the risks causing the vulnerabilities

iii What are some of the attacks carried out on cloud computing

iv How do we stop the attacks carried out in cloud computing

v Are there any measures that can be put in place to stop the attacks on cloud computing.

1.7 Significance of the Project

Dropbox is currently the most popular provider of cloud computing services with the numbers rising each and every day (Winder, 2016). Because of this reason and the expected rise, Dropbox is by now responsible for a considerable traffic volume. This project will help the various Dropbox users to be aware of the vulnerabilities present in Dropbox systems and any possible measures that can be implemented to ensure that the data stored on the cloud is safe from alterations and on worst scenarios leakage or loss.

1.8 Scope of the Project

This project will be research based, and will mostly rely on previous works and journals that have been done together with case studies presented regarding cloud computing security structure. I am going to analyze the security features being implemented currently in Dropbox cloud computing, any vulnerabilities present in the system and suggest any best solutions that can be put in place to solve the security problems or issues being experienced.

1.9 Assumptions of the study

My research will be analyzing the security structure of Dropbox cloud computing and go to an extra step to suggest any techniques that can be implemented in the system to solve the security vulnerabilities found. My research will mainly rely on previous work done, surveys and case studies of the same. The research will therefore rely on both primary and secondary data collected from group of users. It will therefore be assumed that the data collected previously will be a representative enough for generalization.

CHAPTER TWO
LITERATURE REVIEW

According to Rountree and Castrillo (2014), despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring. The common challenges include data protection and data recovery and availability.

Data Security/protection is a crucial element that warrants scrutiny (Rountree & Castrillo, 2014). Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers which are owned by enterprises protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them (Rountree & Castrillo, 2014).

In data recovery and availability, all business applications have Service level agreements that are stringently followed (Rountree & Castrillo, 2014). Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support

i Appropriate clustering and Fail over
ii Data Replication
iii System monitoring (Transactions monitoring, logs monitoring and others)
iv Maintenance (Runtime Governance)
v Disaster recovery
vi Capacity and performance management

If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe (Rountree & Castrillo, 2014).

According to Cloud Security Alliance (CSA), over 70 percent of the world's businesses now operate – at least in part – on the cloud. With benefits like lower fixed costs, higher flexibility, automatic software updates, increased collaboration, and the freedom to work from anywhere, 70 percent isn't a big surprise.

Still, the cloud has its share of security issues. Recently the Cloud Security Spotlight Report showed that 90 percent of organizations are very or moderately concerned about public cloud security. These concerns run the gamut from vulnerability to hijacked accounts to malicious insiders to full-scale data breaches. Although cloud services have ushered in a new age of transmitting and storing data, many companies are still hesitant or make the move without a clear plan for security in place. We'll show you a big picture view of the top 10 security concerns for cloud-based services you should be aware of.

Kurtz and Vines, state in their book that well-known security experts decipher the most challenging aspect of cloud computing-security Cloud computing allows for both large and small organizations to have the opportunity to use Internet-based services so that they can reduce start-up costs, lower capital expenditures, use services on a pay-as-you-use basis, access applications only as needed, and quickly reduce or increase capacities (Kurtz & Vines, 2015).

Kurtz & Vines discuss the extremely challenging topics of data ownership, privacy protections, data mobility, quality of service and service levels, bandwidth costs, data protection, and support. As the most current and complete guide to helping you find your way through a maze of security minefields, this book is mandatory reading if you are involved in any aspect of cloud computing. Coverage Includes: Cloud Computing Fundamentals Cloud Computing Architecture Cloud Computing Software Security Fundamentals Cloud Computing Risks Issues Cloud Computing Security Challenges Cloud Computing Security Architecture Cloud Computing Life Cycle Issues Useful Next Steps and Approaches (Kurtz & Vines, 2015).

According to Winder Dropbox dropped the ball back in 2012 as far as security was concerned when it admitted that a compromised password had been used to access an employee Dropbox account which gave access to a document containing some user email addresses which then got spammed (Winder, 2016).

There is an attack known as man in the cloud attack that has been carried out on Dropbox accounts. According to (Peters, 2016) black hat USA Las Vegas, using no malware or stolen credentials, attackers could obtain complete access to a user's Google Drive or Dropbox account, steal data, and corrupt legitimate files with malicious code to infect target users. It's called a man-in-the-cloud attack, and is undetectable by both perimeter and endpoint security tools (Peters, 2016). Researchers at Imperva here today released details about the attack. Attackers can compromise cloud file synch services like Google Drive, Dropbox, One Drive, and Box. This can be made possible by say the attacker stealing a user's account credentials or through the back door where the attacker compromises the server, but rather through a side hatch: the user's endpoint machine (Peters, 2016).

To synch files between the endpoint and the cloud, the service first makes the user authenticate, then hands them synchronization token and stores it on the endpoint. The token can be used on multiple machines. So all the man-in-the-cloud attacker needs to do is steal a copy of that synchronization token. As Imperva has discovered, they can do that by convincing the user to run some very typical code that won't raise any red flags. Instead of using noisy malware, they just make a few basic, and temporary, configuration changes (Peters, 2016).

In the current information communication and technology world, there is a new trend whereby organizations and other individual users are trying their best to ensure that they have access to their information from anywhere in the world provided they have access to internet (Winder, 2016). This is also being used from another view of backing up your data and any crucial information. This is where cloud computing comes in. Cloud computing commonly known as cloud storage is whereby information and data is stored in data banks online which enables the users to retrieve the data anytime and from anywhere.

According to Winder, (2016) Cloud computing is playing a great deal in data storage and providing backup services to users and organizations in general. As a result, cloud computing has gained increased popularity among the users. There are also organizations providing commercial cloud services while there are others providing free storage services depending on what the user wants (Winder, 2016).

CHAPTER THREE
METHODOLOGY

3.1 Introduction

The main aim of this study is to analyze the security vulnerabilities present in Dropbox cloud computing and suggest any possible measures that can be implemented to counter the vulnerabilities present in the system. The research will extensively use various categories of data extracted from previous literature pertaining to Dropbox cloud computing. This research project will also implement a review of the literatures.

3.2 Research Strategy

The study involved collecting data from various sources, including qualitative surveys and statistical publications, case studies and previously published works (meta-analyses). This research will implement the use of a qualitative study model (Lapan, et al 2012). It will implement the use of case studies regarding previously reported security cases regarding Dropbox cloud computing.

3.3 Research Design

The research design is used to state the conceptual structure within which the research would be conducted. The design enables the research to be as efficient as possible and to be in a position to yield maximum information. In other words, the design is used to provide for the right techniques to be used in data collection with minimal expenditure of effort and money. The research design will rely on the research purpose. This is a descriptive research and the researcher will implement case studies and surveys to be able to achieve my desired outcome (Newby, 2013).

Descriptive research is a process of collecting data in order to test hypotheses to answer questions concerning the current status of the subject under study. Descriptive research is used to ascertain and describe the characteristic of variables of interest in a situation. This kind of research is mostly undertaken in organizations to learn about and to be in a position to describe characteristics in a group.

3.4 Research Approach

The research is going to utilize qualitative research approach. This form of approach is concerned mostly with subjective assessment of attitudes, opinions and behavior. In this form of approach the research relies on the researcher's insight and opinions. Qualitative is mostly concerned with the phenomenon relating to the quality of something by quantifying it on two bases that is the presence or absence of something (Lapan, et al 2012).

The reason as to why this researcher chose this form of research approach is because my research will be an analysis of the security structure of Dropbox cloud computing. In order to achieve the intended purpose of this research it will be using previous works that had been done and journals. From this point of view, the researcher will be in a position to determine how secure data in Dropbox cloud is, basing it as good or bad. As a result, qualitative approach was best suited for this research.

One of the main delimitation of this form of research approach was that, it produces a generalized view on certain aspects of the research (Lapan, et al 2012). As a result it will tend to make generalized conclusions especially where a small population was in question. The reliability of the research might therefore be compromised especially when using large populations.

3.5 Data Collection

This aspect begins after defining of the research problem and the research design. Data collection will be quite an important aspect of my research (Kothari, 2004). Generally there are two types of data, primary data and secondary data. This research will rely on secondary data. Secondary data is data that has previously been collected by another researcher and it has been successfully passed through the data statistical process.

Because the research project is using secondary data form, the researcher must look into various sources that have the required data regarding security status of Dropbox cloud computing. These data sources will include publications both from the government and from private researchers or international bodies, books, magazines, newspapers, reports, public records and statistic and finally other sources of published information.

Considering the nature of this research, secondary data would be best suited for it, whereby it will be in a position to analyze the data acquired to come to a particular conclusion. However, there is a major delimitation of this form of data whereby there is a large number of unpublished materials that may pose a danger of giving misleading data to the researcher (Kothari, 2004).

The method used in data collection would be case study method. According to Kothari, (2004), the case study method is a technique by which individual observes carefully a particular unit in relation to other units. This is a popular form of qualitative analysis where the study is done in depth. In my research I will take a close look at the security incidences in Dropbox cloud computing, compare them with other institutions offering cloud services and how the incidences were dealt with (Kothari, 2004).

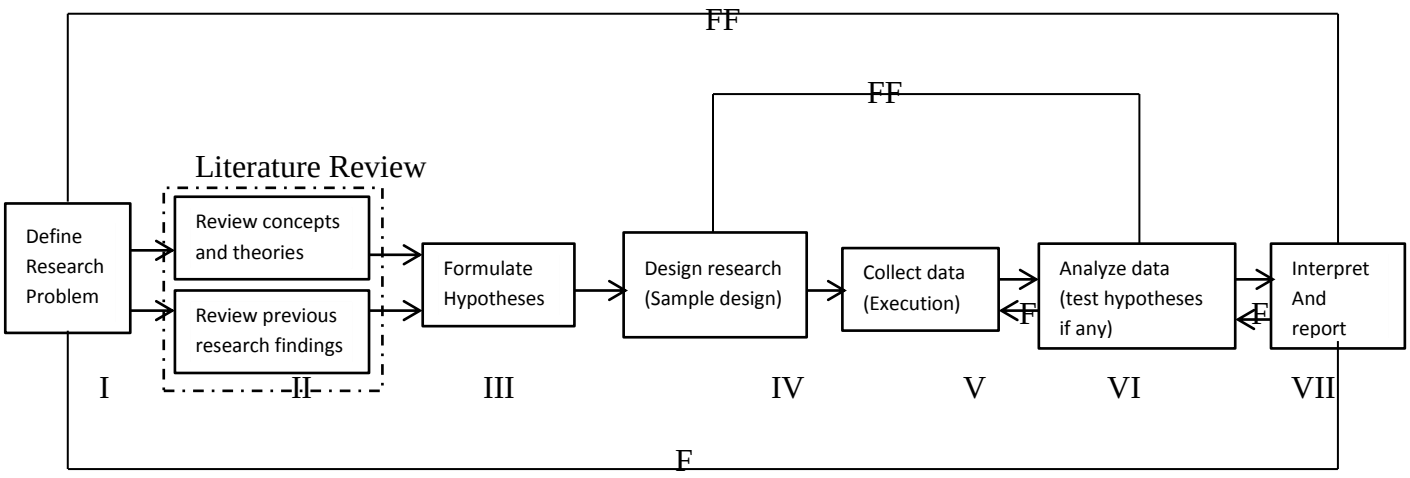
3.6 Sample Selection

According to Kothari, (2004) sample selection is defined as a definite plan for obtaining a sample from the sampling frame. It refers to the technique or the procedure the researcher adopted in selecting some sampling unit from which inferences about the population was drawn. The method of sampling used in this research was purposive sampling whereby sample members are selected on the basis of their knowledge to the research topic, not forgetting their relationship and expertise to the subject.

3.7 Research Process

This consists of the series of action or steps necessary to effectively carry out research and the desired sequencing of these steps. The research process can be summarized by the following chart.

Research Process in Flow Chart



KEY
F – Feedback (Helps in controlling the subsystem to which it is transmitted)
FF – Feed Forward (Serves the virtual function of providing criteria for evaluation)

Fig 3.1. Research Process in Flow Chart

3.8 Data Analysis

After the data has been collected, the researcher turned to the task of analyzing it. Descriptive and inferential statistics were the man methods used since the data collection was in qualitative form. The data analysis and presentations of the data focused on the frequencies tables and percentages (Kothari, 2004).

3.9 Ethical Consideration

This research should ensure that it is up to the ethical obligations to pursue valid knowledge. This is to ensure that the research is of high quality in that it does not waste resources and does not offer misleading information that might potentially affect the users of Dropbox and cloud computing services in general (Rosnow & Rosenthal, 2005).

This research should not offer deceiving information. Deception occurs in two ways, active deception and passive deception. Active deception is deception by commission that is adding information that is not true in nature while passive deception is deception by omission whereby it occurs by the researcher leaving out important information (Rosnow & Rosenthal, 2005).

This research project will ensure that all ethical standards in research are followed including ensuring that there is no plagiarism in my work whether intentional or accidental.

3.10 Research Limitations

This research will rely on the use of case studies. However, there exist a number of assumptions that must be considered while using case study method. For instance, the assumption on the uniformity of human behavior while in the real sense, human behavior vary a lot from one person to the other. There was also the assumption that comprehensive study of the unit concerned was done. This therefore implies that the data used was a complete and the analysis done.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

This chapter presents the study data on the security vulnerabilities present in Dropbox cloud computing. The data was collected from case studies and previous works done in this area of study. Findings will be interpreted with frequencies and percentages with presentation done using graphs and tables. Data findings will then be linked with the researcher's opinion as well as the existing body of knowledge for the elaborate interpretation and discussion. This chapter is organized in sections beginning with an analysis of case studies collected followed by an analysis of any previous works done regarding cloud computing security.

4.2 Overview of Cloud Computing Security

The growing demands of business and the competition in the provision of services has led to many enterprises outsourcing IT provision using cloud computing to handle business processes and data management. Ideally, the benefits that are offered by cloud computing technology can accommodate the rapidly increased demands of the organizations and individual customers. However, the usage of cloud computing has potential security concerns (Naser, et al 2015).

Migrating an on-premise application to the cloud may present the enterprise with a number of security risks and threats like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands. Making sensitive information available on the internet requires a considerable investment in security controls and monitoring access to the content (Marg, 2016). In the cloud environment, the enterprise may have little or no ability to store or backup processes and, as the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of file access and deletion becomes a significant challenge.

Organized criminals and hackers see this as a new frontier to steal private information, disrupt services and cause harm to the enterprise cloud computing network. Internet browser is the first stage where security measures should be implemented because vulnerabilities in the browser open the door for many follow-on attacks. Security has therefore been indicated as the biggest for public cloud adaptation (Marg, 2016).

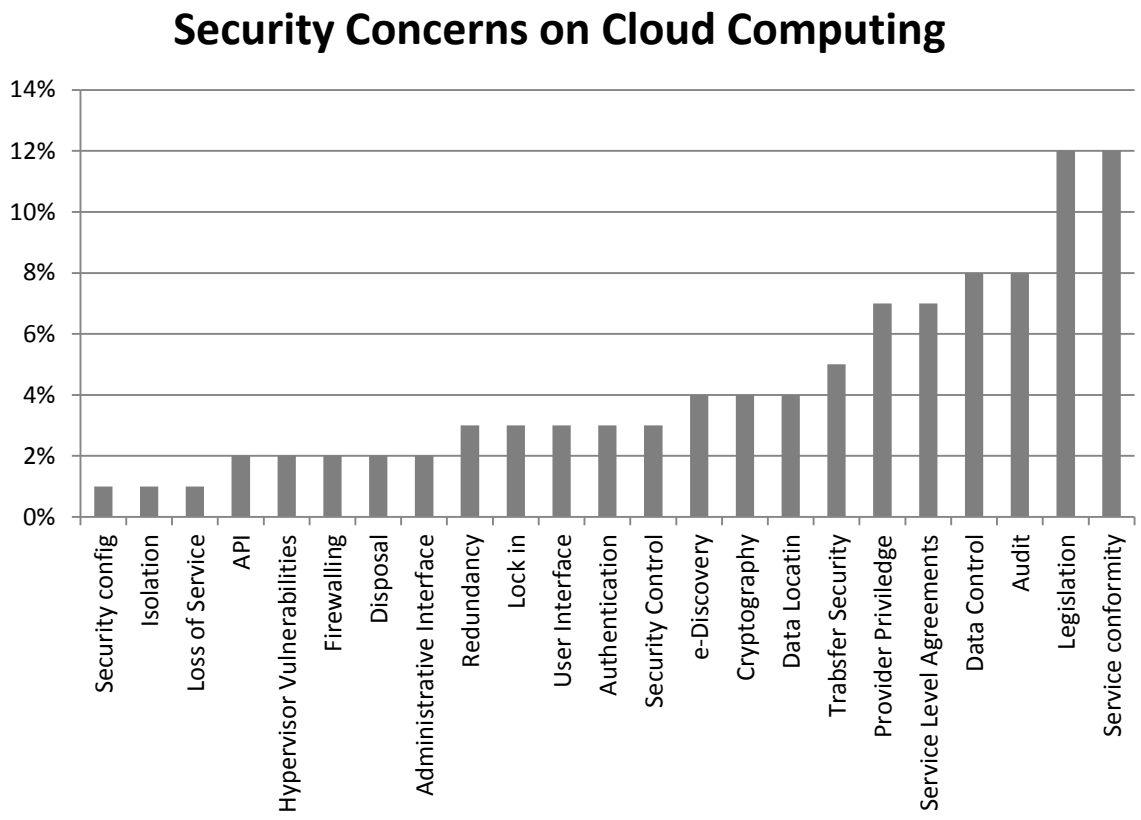


Fig 4.1. Security Concerns on Cloud Comp

Marg (2016) predicts that by 2020, 95 percent of cloud security failures will be due to fault at the customer's end. This means the technology will be strong and secure and that the only way data can be compromised is due to lack of understanding at the user side.

4.3 The CIA Triad in Cloud Computing

Information security is measured using three parameters. These are confidentiality of data, integrity and availability of the data. I am going to analyze the three parameters in regards to cloud computing

i Confidentiality

Confidentiality refers to the privacy of the data stored in a system. Measures undertaken to ensure confidentiality of data in cloud storage are designed to prevent the data from being accessible by the wrong people and ensuring only the right people are in a position to access the data. This therefore ensures that accessibility of the data is restricted (Chou, 2013).

According to Chou, (2013) some of the methods used to ensure data confidentiality in cloud storage include data encryption, user ID and password as a two factor user authentication. There is also the implementation of Simple Object Access Protocol (SOAP) messages that are transmitted through HTTP protocol with an Extensible Markup Language (XML) format when a client requests services to a web server through a web browser. In order to ensure confidentiality and data integrity of SOAP messages in transit between clients and servers, a security mechanism, Web Services Security, for web service is applied. It uses digital signature to get the message signed and encryption technique to encrypt the content of the message. This makes the client authenticated and the server can validate that the message is not tampered with during transmission (Chou, 2013).

ii Integrity

This entails maintaining the consistency, accuracy and trustworthiness of data in the cloud. Data must not be changed while being uploaded to the cloud storage, during storage or even during retrieval. Cloud storage service providers should ensure that steps and measures are put in place to ensure that data cannot be altered by unauthorized people other than the owner of the data (the user). In order for cloud storage service providers to ensure that there is data integrity, measures such as file permissions and user access control are being implemented. Version controls have also been implemented to protect erroneous changes or accidental deletion by authorized users. There has also been a measure of detecting changes in data caused by non-human events such as an electromagnetic pulse (EMP) or server crash (Chou, 2013).

iii Availability

Availability can be defined as a design by which the downtime of systems, network, storage and infrastructure are standardized thereby assuring uninterrupted services to its stakeholders. Typically, the availability is reported as number of nines. For example, six nines 99.9999% means a downtime of 31.5 seconds a year and four nines 99.99% means a downtime of 52.56 minutes a year. A definition of high availability also takes into account the system down time due to scheduled maintenance (Marg, 2016).

In order to ensure that systems in a cloud are always available, survival against multiple levels of failures should be designed. In case of IaaS, the high availability aspects are driven more from a hardware point of view to keep the systems in a healthy state. In other delivery models it is viewed from a software point of view like unavailability of services is related to downtime of applications deployed on the cloud, and unavailability of data is related to the downtime of associated storage infrastructure (Marg, 2016).

4.4 Dropbox Security Incidences

According to Wu, et al (2015) Drop box is being used by more than 200 million users. Its ability to seamlessly provide cloud storage with minimal user complexity is the key for its wide spread popularity. Despite of its high usability, Drop box has been recently criticized for loose ends in security (Wu, et al 2015). Security and usability is not always mutually exclusive, and we believe there is still a lot of room to improve Drop box's security without affecting the unique user experience. In this paper, we present a RAM analysis based method to extract the key security token for account access. In addition, we describe a new technique to bypass authentication and gain unauthorized access to Drop box accounts by using the new tray login feature on the most current Drop box client v2.4.x.

Dropbox is used by an estimated 70% of businesses, according to Osterman Research. These companies presumably access, synchronize, and share information stored on the Dropbox cloud servers. However, industry experts have pointed out that Dropbox has security limitations and risk factors that make it an unsuitable application, especially for enterprise organizations (Wu, et al 2015).

4.5 Dropbox Security Concerns

In this research the following security concerns were reported in Dropbox cloud computing (Topal, 2016):

1. IT has no control or visibility.

In Dropbox cloud storage, IT administrators or users cannot control who can sync files. This is a feature that exposes data to unauthorized access and modifications. This inability to set granular read/write permissions to directories and files is a severe limitation for businesses. The condition is made worse by limited encryption features.

2. You can't set different sharing permissions for sub-folders

Dropbox cloud lacks the functionality of setting access permissions to sub-folders. In business requirements, this is a common feature but it is not available on Dropbox cloud storage. In order to achieve this feature, the user needs to change the structure of the folders.

3. Users can't set granular permissions

Dropbox lacks the functionality of specifying how to share data. Individuals and companies share data differently. Project collaboration should be limited to specific people sharing specific files.

4. You can't share password-protected web link

Password protected files are supposed to be shared in the form they are, in that they should be transmitted in this protected nature. However, once the files are sent via Dropbox, the protection is removed hence subjecting the files to a great security risk during transmission.

5. No remote data deletion

In the current information world, data theft is a serious issue. This happens where a group member's laptop or computer is stolen. Dropbox does not provide for remote data deletion in case of theft of machine occurs.

6. No data locking during editing

Dropbox does not provide for the feature of locking a file during editing/modification. This subjects the data to a large risk especially when the user is editing a number of files simultaneously.

7. No log Files

Dropbox does not provide a log file showing a track of how files and data has been changed/modifies or accessed. This is a major security problem because the user might not be aware of any activities carried on in his account without his knowledge.

8. You can't lock files for collaborative editing

Many cloud servers enable users to share links with others for the purpose of collaboration and file sharing, but Dropbox allows anybody who discovers this link to access the data. People who find the link need not be registered users.

4.6 Reported Security Cases

In 2012, August Dropbox acknowledged that they had been hacked. This happened through spam mailings afflicting users when hackers used passwords obtained from third party sites to access a number of Dropbox accounts. According to Agarwal (2016) it was found that usernames and passwords stolen from other websites were used to sign in to a number of Dropbox accounts.

There was also another case whereby a stolen password from an employee in Dropbox was used to access employee accounts containing project documents and user email addresses. As a result of this attack, Dropbox started offering a two factor authentication option alongside providing a new web page to let Dropbox account holders check out accesses to their accounts. Users were also required to ask for new passwords for all their accounts to boost security (Darrow, 2016).

4.7 Top Dropbox Customer Complaints

According to a survey done by FixYa, cloud based file storage is becoming the expected method for sharing data, both personal data and data relating to organizations. The survey uses volunteer staff to help with technical support information on its website (Mearian, 2016). The information is designed to help consumers repair and troubleshoot product problems by them. The survey uncovered some of the common problems in cloud storage, such as synchronization problems in five major companies offering cloud storage services.

Of the five cloud storage companies sampled in the research, Dropbox appeared with the highest number of security issues reported, with Google Drive following with 30% of the respondents reporting missing folders. According to Mearian, (2016) Dropbox has suffered a couple of security issues. Apart from the 2012 hacking, there has been a problem with privacy security settings as well. There has also been a reported case in 2011 where accounts could be accessed without user passwords. This led to the breach of user confidentiality where the files and data stored in the cloud storage could be accessed by other people due to the privacy settings problem (Mearian, 2016).

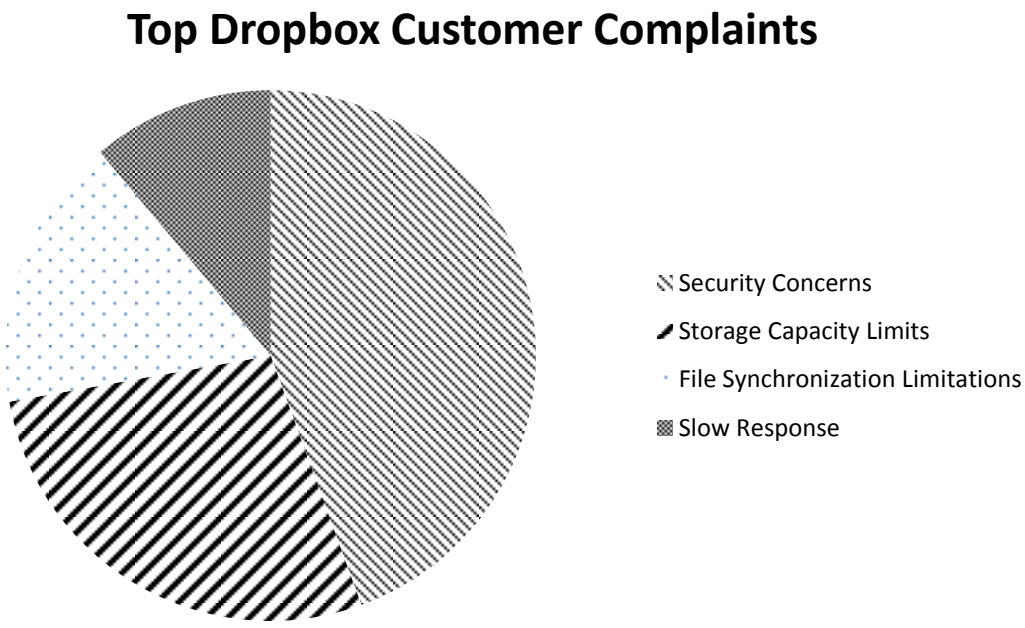


Fig 4.2. Top Dropbox Customer Complaints

CHAPTER FIVE

SUMMARY

5.1 Introduction

This chapter will discuss a summary of the findings in my research regarding security vulnerability in Dropbox cloud computing relying on the data collected from previous scholarly works and reported cases regarding the security status of Dropbox.

5.2 Summary of Findings

Relying on the objectives of research, a summary of each objective is going to be given.

Table 5.1 Summary of Findings

Objective	Findings
To analyze security vulnerability in Dropbox and some of the causes (Threats)	Some of the security vulnerabilities in Dropbox cloud computing include: i Buffer overflows ii Injection vulnerabilities iii Sensitive data exposure iv Broken authentication and session management v Security misconfiguration Some of the security threats in Dropbox cloud computing include i Abuse and evil use of cloud computing ii Insecure API iii Malicious insider iv Shared technology vulnerability v Data loss/leakage vi Account, service and Traffic hijacking

To identify some of the attacks that have previously been carried out on Dropbox and how they can be stopped	Some of the major security attacks I Dropbox include: i Man in the middle attack (man in cloud attack ii Denial of service attack iii Distributed denial of service iv Phishing attack v Account hijacking vi Malware injection vii Social engineering attack viii Traffic flooding
Suggest some of the ways a user can ensure security of their data and information stored in Dropbox cloud	These are some of the security aspects that can be carried out to address the threat of cloud computing i Choose a strong password ii Enable two step verification iii Adjust security settings iv Monitor account activity

CHAPTER SIX
CONCLUSION AND RECOMMENDATION

6.1 Introduction

This chapter, will conclude this research and give recommendations on how to improve the security status of Dropbox cloud computing. It will draw a conclusion of the study, make recommendations and propose any further areas of study related to this study.

6.2 Conclusion

From the study conducted, the following conclusions were made from the findings.

During the study, it was clear that Dropbox has suffered and number of security issues which were higher in Dropbox than other companies offering cloud computing services. However, this does not mean that Dropbox is unsecure, mutual security incidences exist among the cloud storage services. The good thing is that Dropbox is quick to react to the problem and solutions are meat as quick as possible and improvements made. For instance after the 2012 hacking, the security of Dropbox account was improved with users being required to request for a new password and a two-step security authentication process was put in place to increase the level of security.

Finally, data security in cloud computing must necessarily be safeguarded when processing personal data. Confidentiality, availability and integrity of data must be ensured by means of appropriate organizational and technical measures. This also includes the protection of systems data from the risks of unauthorized or arbitrary destruction, loss, technical faults, forgery, theft and unlawful use including unauthorized modification.

6.3 Recommendation

In relation to the study, the researcher would recommend that Dropbox users and cloud computing users should ensure that they also ensure security to their cloud accounts. Among the things they should do to ensure they improve the security of their data and accounts in general include:

i Choose a strong password to your account
ii Enable two steps verification which adds extra protection to your account.
iii Adjust security settings to reduce the number of linked devices
iv Monitor your account activity

6.4 Future works

Further research can be done in the following areas as regards to this area of study

i Identifying the best cloud security standard
ii Security improvements made to cloud storage services
iii Major security problems in Google Drive

REFERENCES

Agarwal, A. (2016). *Security update and new features*. *Dropbox Blog*. Retrieved 16 November 2016, from https://blogs.dropbox.com/dropbox/2012/07/security-update-new-features/

B. Wu, T. Nguyen and M. Husain, "Implementation Vulnerability Associated with OAuth 2.0 – A Case Study on Dropbox," *2015 12th International Conference on Information Technology - New Generations*, Las Vegas, NV, 2015, pp. 135-138.

Chou, T. (2013). Security Threats on Cloud Computing Vulnerabilities. *International Journal Of Computer Science And Information Technology*, *5*(3), 79-88. http://dx.doi.org/10.5121/ijcsit.2013.5306

Darrow, B. (2016). *Gigaom | Dropbox: Yes, we were hacked*. *Gigaom.com*. Retrieved 16 November 2016, from https://gigaom.com/2012/08/01/dropbox-yes-we-were-hacked/

Groves, R., Fowler, F., Couper, M., Lepkowski, J., Singer, E., & Tourangeau, R. (2009). *Survey methodology*. Hoboken, N.J.: Wiley.

Hay, R. (2015). *DroppedIn: New Vulnerability Discovered in Dropbox SDK for Android*. *Security Intelligence*. Retrieved 17 October 2016, from https://securityintelligence.com/droppedin- remotely-exploitable-vulnerability-in-the-dropbox-sdk-for-android/

Jajodia, S. *Secure cloud computing*.

Kothari, C. (2004). *Research methodology* (1st ed.). New Delhi: New Age International (P) Ltd.

Kurtz, R. & Vines, R. (2015). *Cloud security* (20th ed.). Indianapolis, Ind.: Wiley Pub.

Lapan, S., Quartaroli, M., & Riemer, F. (2012). *Qualitative research*. San Francisco: Jossey-Bass.

Marg, N. (2016). *Consultation Paper on Cloud Computing* (1st ed.). New Delhi: Telecom Regulatory Authority of India.

Marinescu, D. (2013). *Cloud computing*. Boston: Morgan Kaufmann.

Mearian, L. (2016). *The top 5 issues with the top 5 cloud storage services*. *Computerworld*. Retrieved 16 November 2016, from http://www.computerworld.com/article/2493144/cloud-computing/the-top-5-issues-with-the-top-5-cloud-storage-services.html

Naser, S., Kamil, S., & Thomas, N. (2015). A Case Study in Inspecting the Cost of Security in Cloud Computing. *Electronic Notes in Theoretical Computer Science*, *318*, 179-196.

Newby, P. (2013). *Research Methods for Education*. Hoboken: Taylor and Francis.

Peters, S. (2016). *Man-In-The-Cloud Owns Your Dropbox, Google Drive -- Sans Malware*. *Dark Reading*. Retrieved 19 October 2016, from http://www.darkreading.com/cloud/man-in-the-cloud-owns-your-dropbox-google-drive----sans-malware-/d/d-id/1321501

Rosnow, R. & Rosenthal, R. (2005). *Beginning behavioral research* (5th ed.). Englewood Cliffs, NJ: Prentice Hall.

Rountree, D. & Castrillo, I. (2014). *Basics of cloud computing*. Amsterdam: Elsevier Syngress.

Wang, L. (2012). *Cloud computing*. Boca Raton, FL: CRC Press.

Sanders, J. (2014). *Dropbox and Box leak files in security through obscurity nightmare-TechRepublic*. *TechRepublic*. Retrieved 17 October 2016, from http://www.techrepublic.com/article/dropbox-and-box-leak-files-in-security-through-obscurity-nightmare/

Schwartz, M. (2012). *5 Dropbox Security Warnings For Businesses*. *Network Computing*. Retrieved 17 October 2016, from http://www.networkcomputing.com/cloud/5-dropbox-security-warnings-businesses/862532134

Singh, Y. (2006). *Fundamental of research methodology and statistics*. New Delhi: New Age International.

Topal, J. (2016). *6 Reasons Why Dropbox Isn't Secure Enough for Business*. *Business 2 Community*. Retrieved 25 November 2016, from http://www.business2community.com/cloud-computing/6-reasons-dropbox-isnt-secure-enough-business-0795298#xSO8iHRymIF3QwHa.97

Winder, D. (2016). *How secure are Dropbox, Microsoft One Drive, Google Drive and Apple iCloud cloud storage services?*. *Alphr*. Retrieved 25 October 2016, from http://www.alphr.com/apple/1000326/how-secure-are-dropbox-microsoft-onedrive-google-drive-and-apple-icloud-cloud-storage