International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

Securing File on Cloud Computing System using Encryption Software: A Comparative Analysis

Victor O. Waziri, John K. Alhassan, Ismaila Idris, and Raji Abdullahi Egigogo
Cyber Security Department, Federal University of Technology Minna, Nigeria
victor.waziri@futminna.edu.ng

***Abstract*—The need for an efficient, secure, accurate, reliable way of securing user information arises as individuals and organizations increase their dependency on cloud computing. Data encryption is very important nowadays due to increasing in data theft not only on cloud platform but also on user's computer. For this study, 3 different Open Source encryption software's (7-zip, B1 Free Archiver and Axcrypt) were tested for their encryption type, usability, advantages, accessibility and others, all of which were found to be using AES 256-bit Algorithm for encryption due to its reliability. 7 zip is the most preferred encryption program due to its wide availability, light weight, faster encryption and better compression ratio. To ensure the security of information, encryption of sensitive data not only to be uploaded to the cloud but also on user's computer becomes necessary.**

Keywords-cloud; 7-zip; B1 Free Archiver; Axcrypt

I. INTRODUCTION

The delivery of computing services across the globe is cloud computing [1]. Cloud facilities allow persons and companies to use hardware and software that are handled by third parties at inaccessible locations [2]. There are services provided by the cloud such as webmail, online file storage, online business applications and social networking sites among others. The cloud computing model permits access to computer resources and information from everywhere that a network connection is available. It also offers a shared pool of resources, including computer processing power, networks data storage space, specialized corporate and user applications [3].

A common reoccurring word in cloud computing is the internet. The Internet is a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for the geographic location [4].

It is a worldwide system of unified networks of computer that use the(TCP/IP) that is internet protocol suite to join billions of devices worldwide, consisting of millions of academic, private, business, public, and government networks of local to global scope, coupled with a wide array of wireless, optical networking technologies and electronic devices [5].

In cloud, privacy and security of personal information is very important. Often in another country, personal information is turned over to another organization making it unsecured. It is essential to ensure that data is only accessed by the authorized user to overcome the high level of insecurity [6]. For businesses, organizations and individuals that are in view of using a cloud services need to know the privacy policies, understands the security and practices of the cloud providers.

The complexity and cost of operating and owning computers and networks is significantly reduced when using cloud computing. For example If an individual or company uses a cloud services, less money is needed and spent on buying software licenses or hardware or even information technology infrastructure

One of the major cloud service providers Microsoft is committed to providing a cloud you can trust. They believe there are five critical areas you need to know about when talking about cloud security [7]:

- Security options and capabilities available in the cloud
- Maintaining privacy and control of your data
- Addressing industry compliance rules
- The need for transparency and visibility into how your data is stored and protected.

Several literatures have proposed various method of ensuring the security of data in cloud such as authentication, accesses controls and cryptography among others which are mostly enforced either by third parties or service providers. The paper proposed a technique of securing files on cloud using encryption program by suggesting the best amongst the three presented based on the comparison made.

The paper is structured in the following manner. The first segment is the introduction which contained motivation, aim, objectives, scope and limitation of the research. The next segment reviewed several literatures that are related to the subject matter in details. In Section III, methodology used in evaluating and testing the software's is discussed. The main activities involved in evaluating the three (3) selected progra m and a comparative analysis of the selected programs were explored in Section IV. Finally, the paper is completed with the succeeding segment.

A. Motivation for the Research

Today, numerous organizations that offer cloud technologies include among others Amazon, Google,

Dropbox and Microsoft with new once coming up every now and then. Every of these cloud providers come with its own kind of services and different security technologies that strive to convince the customer of it been the best either way.

It will be wiser if the security of information is placed more in the hands of the owner as this go along to install and improve the confidence level in cloud security and data integrity since the only person that can easily access information on the cloud must be the same person that puts them or any other party granted access by the owner of the information. Hence, the motivation for this research came as result of the increasing need to have more effective way for securing data on the cloud to keep it away from data theft.

B. Aim and Objectives of the Study

The aim of this research is to implement and test different encryption software platforms and select the one's that will be best suited to use in securing files on the cloud technology. The objectives of the study include to:

- Test for different software encryption (Types/ parameters).
- Employ the use of some encryption software's and implement a means of ensuring security by allowing access to file using password encryption setup by the information owner so that the integrity of the outsourced data is not compromised on the cloud.
- Compare the encryption software's and ascertain the area that is best suited for securing files on the cloud

C. Scope and Limitation

The research covers implementation of some encryption software. Cloud computing system is an internet based application, which makes its accessible from every corner of the world. The research will provide standard and guidelines for the cloud service providers and as well as cloud users.

II. LITERATURE REVIEW

The idea behind a centralized computing began as far back as the 1960s, when mainframe time-sharing technology was the computing services provided across a network. At exactly 1966, a book titled "The Challenge of the Computer Utility" was put out by a Canadian engineer Douglass Parkhill, which traces the idea of computing as a public utility with a centralized computing facility to which many remote users connect over networks [8].

In the 1960s, computing resources were efficiently used by the mainframe time-sharing method and offered acceptable performance to users; As a result of increasingly high hardware costs mainframes were hard to provision up-front and scale. Therefore, users didn't have full power over the performance of mainframe applications as it depended on how many users used the mainframe at a given moment. Thus, with the preface of personal computers users prefer to have absolute power over their computing resources, even although these resources are not efficiently used.

Personal computers became affordable and business deserted mainframes with the change in the semiconductor industry. The challenge of how to share data was then introduced. Client-server systems were believed to tackle this data-sharing challenge through the means of providing centralized data management and processing servers. As the Internet became widely adopted and business computing needs grew, the original simple client-server architecture changed into more compound architectures. Thus, the complexity and the management costs of IT have passed even the costs of real software development in big organizations are typically lesser than infrastructure maintenance and costs of the software.

The dream of numerous enterprises is the background information technology matters and how to focus on core business instead. However, the result of the cloud computing acceptance is yet to be pictured, many companies think that cloud computing may present a feasible alternative model that may cut costs and complexity whereas escalating operational competence.

A. Cloud

The Cloud is a computing platform that depends on the internet for availability and accessibility [9]. The cloud makes it feasible to use information from everywhere at any time. In the case of traditional computer setup, the person accessing the resources is required to be in the same place with the data storage device [10]. This is especially helpful for businesses that cannot afford the same amount of hardware and storage space as a bigger company which makes the cloud cheap and accessible for all.

B. Cloud Computing

[10] defined Cloud computing as a subscription-based service where you can obtain networked storage space and computer resources. A clearer way to understand cloud computing is to relate it to the experience with email. The email client such as Yahoo!, Gmail, Hotmail among others takes care of housing all the hardware and software necessary to support the user personal email account. The authors classified cloud computing into two which are can be based on services offered (infrastructure as a service (Iaas), platform as a service (PaaS) and software as a service (SaaS)) and location (public, private, and hybrid community cloud).

C. Cloud Security

The set of control-based policies and technologies are designed to protect and adhere to regulatory compliance rule in other to enforce overall security in cloud computing, it usage is associated with infrastructure and data applications [11].

The most challenging obstacle to the acceptance of cloud is the security of data. Data is most valuable asset, individuals and organizations are really concern to know the status of their data. That is whether the data is safe or not.

When data are stored internally, individuals, companies, and government are rest assured of its security as they handle the overall control. Even though no warranty that data is more confined within when compared with the public cloud. The public cloud might be even more secured in storing data due to the fact that the providers of these services may implement advance level of security. Various methods of protecting data in the cloud have been implemented but full protection of data cannot be assured. The following are some of the resent techniques proposed by different authors.

A secure and efficient auditing scheme was developed by [12] which have capabilities such as confidentiality, public auditing, maintaining the data integrity and privacy preserving among others. The scheme is made up of three entities: data owner, TPA and cloud server each with its own responsibility. This proposed auditing scheme makes use of SHA-2 for integrity check, RSA signature for digital signature calculation and AES algorithm for encryption.

[15] presented a flexible and efficient distributed method with assured dynamic data support, as well as delete, append and block update. This method support public auditing mechanism and preserving privacy of shared data in the cloud. It involves the hashing technique to achieve the correctness of data across the server in the cloud. The TPA can execute many auditing tasks concurrently.

Two separate algorithms namely symmetric key cryptographic and message authentication code (MAC) generation and was introduced by [16] to support effective storage of data in cloud using public integrity auditing technique. The main research objective was to improve the integrity of the content of data stored in cloud and to reduce the bandwidth. The performance of the scheme was assessed in aspect of block size, time computationa, cycles per block, number of rounds, key size. The evaluation shows that the proposed scheme provides the better results.

[17] proposed cryptographic technique that combines Secure Hash Algorithm 1 (SHA 1) and AES for key generation process and encryption respectively, using a trust computation means for securing the communication amid two servers. This method of trust computation includes the dynamicity of IP address, server rating by users and the number of connection refused.

[18], to ascertain the correctness of users' data in the cloud, an efficient means with outstanding characteristic of data confidentiality and integrity was used. This account presented a clarification which uses the RSA algorithm and the means of hash function beside with different coding tools to give an improved security to the information stored in the cloud. This model cannot completely decipher the hitch of storage of huge data which will grant data access control mechanisms and share data files with integrity and confidentiality.

According to [19], offered a means of providing confidentiality and integrity of the data stored in mobile cloud. The anticipated method uses the RSA algorithm with other decryption and encryption processes so as to ensure that information does not leak on the cloud. In this method, encryption is used to provide security to the data while on transit

[20] proposed privacy preserving public auditing using TPA for security of data files stored on cloud. The proposed method support data partitioning technique for data storage security in cloud service Partitions are again divided into chunks for send at servers this helps to quick retrieval and store. To authenticate the user before gaining access to data so that great level of security achieve, the authors used one time password (OTP) in authenticating the user over network.

[21] proposed a technique that makes use of cryptographic algorithms such as Blowfish, RSA and Digital signature, prevent unauthorized users from accessing the data in the cloud either accidentally or intentionally with the help of Roll Back Access Control (RBAC).

[22], in this paper, the RSA cryptographic method was combined with Magic Square algorithm when implementing data security in cloud computing. The RSA was used to evaluate the local and cloud environment which was analysed with different input file size while magic square deals with complexity in encryption and boosts the security in the cloud environment. The result revealed that encryption and decryption of data using RSA consumed time at an average rate both in the local and cloud environment. It was concluded that RSA algorithm is very secure with the aid of the magic square.

The proposed scheme provides client-side security measure that can be taken to guarantee the information stored in the cloud. The proposal uses the cryptographic techniques of encryption using Diffie-Hellman algorithms and Advanced Encryption Standard (AES). AES was used to encipher the data before uploading to the cloud while Diffie-Hellman algorithm was employed to generate the key pair.

III. METHODOLOGY

This chapter looked into procedures for testing and evaluating the softwares under consideration. These procedures follow a systematically structured approach to effectively understand and provide techniques for the usability and the advantages of the softwares by comparing all standards.

A. Software

The following software's were used to conduct the research:

- 7zip
- B1 Free Archiver
- AxCrypt

These software were selected based on ranking and accessibility offering open source license.

The 7zip was developed by Igor Pavlov 1999. It is an open-source file archiver, an application primarily used to compress files. Also uses its own 7z archive format, but can read and write several other archive formats. The program can be used from a command-line interface, graphical user interface and with window-based shell integration. The cross-platform version of the command line utility 7zip is also available.

B1 Free Archiver is a free multiplatform compression tool and an open-source software project that produces a cross-platform command-line tool and a Java library for creating and extracting file archives in the B1 archive format.

AxCrypt is an efficient, simple, free open source, and easy to use encryption tool. It is a GNU GPL-licensed program for windows which integrates properly with the windows shell. The tool locked a file for a certain period of time and later decrypt itself or if the intended receiver obtained it. AxCrypt proffers security against brute force cracking attempts with a lightweight less than 1MB and supports 128-bit AES encryption only.

B. Considered Implementation of the Software

The following are considered in the implementation of the software.

- Software Encryption Type/Parameters.
- Use of Password protection on files.
- Easy Implementation procedures.
- Comparing the three Softwares and ascertaining the most suitable depending on user need.

C. System Hardware Requirements

The following are the system hardware requirements
A computer system (either desktop or laptop)

- Processor of any kind e.g. Intel Pentium 4.
- 1GB RAM and above.
- At least 200mb Installation Space
- Keyboard.
- Mouse.
- Internet Access

IV. TEST AND EVALUATION

This section deals with the main activities involved in evaluating the three (3) selected programs for the study. The programs were selected due to wide availability, simplicity, and accessibility. System testing involves any activity aimed at evaluating an attribute or capability of a program or system and determining that it meets its required results [13]. It is the installation of the new software after all user requirements are met which basically includes system operating system (OS) and system hardware configuration.

For this study, we made use of Microsoft Windows 7 Professional Edition was used as the OS and a computer system with the following Hardware configurations.

TABLE I. SYSTEM SPECIFICATIONS

Operating System	Microsoft Windows 7 Professional (64-bit)
Type	Laptop
Product Manufacturer/Model	Sony Vaio VPCSA
Processor	Intel Core i7-2640M Processor 2.80 GHz with Turbo Boost up to 3.50 GHz
Ram (memory)	8 GB
Hard Drive	Solid State Drive 256 GB
Graphics Card	Dual Graphics Card (Intel and Radeon Ati)

The Table I shows basic information of the system used during testing and evaluation of the programs. All the programs performed excellently well with no known compatibility issues with the Operating System.

Table II shows that all software's require little space for installation with the highest file size requirement were 140mb.

The table II shows comparative analysis of the 3 selected program based on File Size (64 Bit Installer), File Size after installation on system, open source, version/release date, encryption algorithm, OS compatibility, license, command line interface, self extractor, unlock other encryption, compression ration window Context Menu Integration and Registration.

TABLE II. COMPARATIVE ANALYSIS

	Features	7 zip	B1 free Archiver	Axcrypt
1	File Size(64Bit Installer)	1.31 mb	44.55 mb	7.90mb
2	File Size After Installation on system	4.75mb	140.00mb	5.86mb
3	Open Source	Yes	Yes	Yes
4	Version/Release Date	16.00 (1999-2016)	1.7.122.0 (2015)	2.1.1390.0 (2012-2016)
5	Encryption Algorithm	256 bit AES	256 bit AES	256 bit AES
6	Registration	No	No	Yes (Paid) after 30 Days/ free with 128 bit encryption
7	Windows context Menu Integration	Yes	Yes	Yes
8	Unlock other Encryption	Yes	Yes	No
9	Self Extractor	Yes	No	No
10	Command line Interface	Yes	Yes	Yes
11	License	Free	Free	Licensed
	OS Compatibility	Support all common operating systems (windows,Linux, FreeBSD, mac os, solaris Aix and others)	Support for operating systems (Windows, Linux, Mac and Android)	Windows mainly little functionality for mac osx

The study revealed that 7 Zip is a lightweight application with just 1.31 megabytes (MB) of installation file size in a 64-bit version. It is the most compatible with all the three application used during this research with wide support for almost all common operating systems (windows, Linux, FreeBSD, Mac Os, Solaris and Aix among others). It is an opens source application under the Great New Utility (GNU) and Lesser General Public License (LGPL); therefore 7-Zip can be used on any computer, including a computer in a commercial organization. 7zip support 256bit AES Encryption Algorithm which is still currently unbreakable except using brute force attack which is only easy and possible if password set is not strong enough. i.e using only small length numbers and alphabets with no capitalization and other characters as a password. Even after installing the software the file size is still comparatively smaller than the others. 7zip support self-extraction this implies that a zip file can be created using 7zip that can extract itself without needing any zip manager or 7-zip been installed preinstalled on the system. It is the only one amongst them that support this feature. Some computer hardware vendors install 7zip on their machine during factory installation showcasing its wide acceptance and usability. For software developers and command line gigs 7 zip support command line interface which can be easily integrated into other software for usability within the software's and also since it is an open source, developers are free to lookup the source code to add, modify and make the application better and more suitable for the purpose they require it to perform. It integrates very well with windows operating system and provides easy access through the windows context menu.

7zip can be easily downloaded from the website and has basic windows installation requirement to install. Figure 1 shows a graphical representation of 7zip download website.

Download website: http://www.7-zip.org/download.html

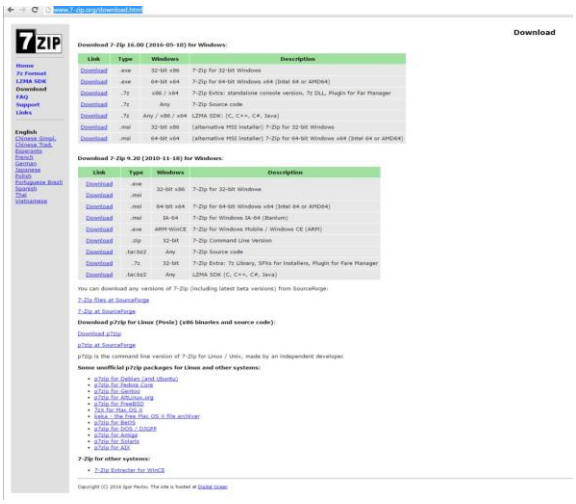

Figure 1. 7-zip Download Page

The software requires a very simple installation process. When running the installer, is run, it simply pops up an installer windows with the default Program file directory where the software is going to be installed to, alternatively, the default directory if so desired during the installation process.

A. *Encrypting File with 7-zip*

The graphical representation on Figure 2 is been labeled with a number to provide the reader with easy reference to the part of the program been explained. This allows the reader pictorial and graphical representation of the program which foster easy comprehension and retention. Though bearing in mind the most important part of the research (encryption), effective use the software from the interface is performed the following after running the software.

- Navigate to the Directory where the file to be Encrypted resides.
- Select the File or Files to be Encrypted
- Click on the Add Button (A new Popup window appears showing you all the possible Encryption parameter possible on the software).
- This represents the encryption parameters that can be choosing, for the purpose of the default parameters provided by the system was used.
- 7z extension is the default file type for 7zip Archive/Encryption, the extension changes when another Archive format is selected (.zip .tar .gzip and others), every of which has its drawback and advantage. Also, the extension file can be .exe telling you option 7 from the graphic is selected representing Self-Extracting Archive (SFX). SFX are archives that can extract themselves without requiring any preinstalled archive or extraction software.

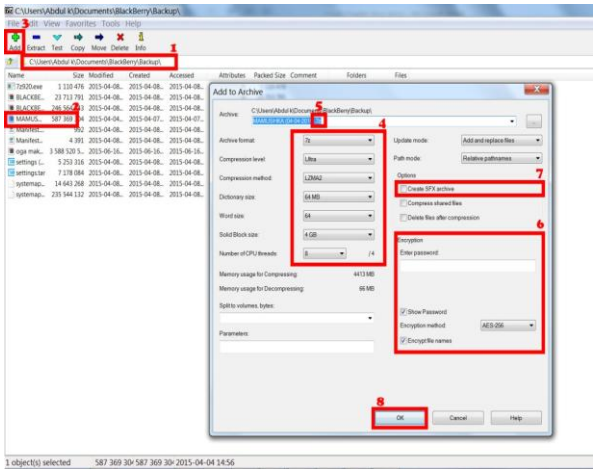

Figure 2. 7zip user Interface after Installation

- This is the most important aspect of the Encryption were password is set to protect the archive from unauthorized access. Without this option been setup, the archive is just a normal archive that can be easily accessed by anyone. Around it, a select box that shows the kind of Encryption system been used (AES 256) which till date is one of the strongest encryption system known.
- This provides option for SFX as earlier discussed in number 5.
- After everything is setup and looking ok. This option commits the selection and proceeds with the archiving. The archived file is by default placed in the same directory as the navigated directory in 1, except if new directory is re-specified by the user.

B. *Archiving a File Using the Context Menu*

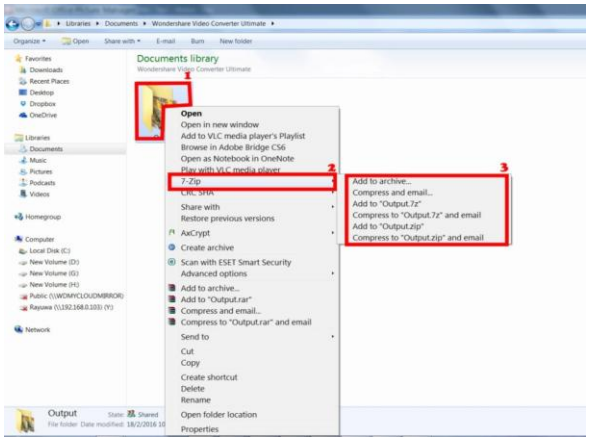

Figure 3. Archiving a file using the context menu

Below are procedures of Creating an Archive (Encryption from the Windows Context Menu). The contexts menu provides a fast and easy way of creating Encrypted Archive.

- Right-click on the desired file/files, folder/folders or a combination of both to be encrypted.
- Select the 7-zip option on the context menu to display other options

- Click on "Add to Archive" to pop up the Encryption option as earlier covered. If basic Archive requires without encryption quickly do that by selecting add to (Filename).7z" or "(Filename).zip".

C. *Extracting file from the context menu*

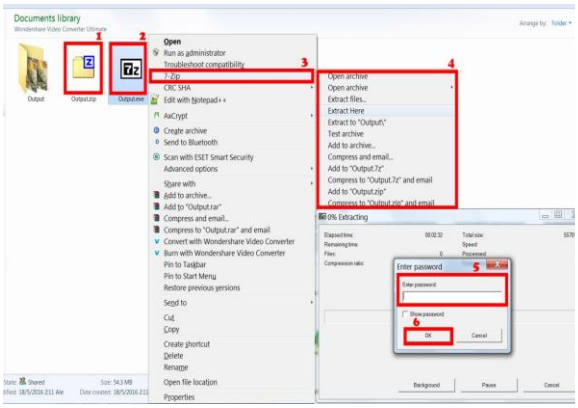

Figure 4. Extracting file using the windows context Menu

If 7zip is setup as the default zip managing software then you can see a file type like the one labeled 1 on the figure 4.

- 7zip Archived file
- 7-zip SFX file
- Right click on the file or files you wish to extract and scroll down to 7-zip and select
- Select the option most suitable to you. Open Archive, Extract Files..., Extract Files Here all pops up a new window demanding for password used in setting up the Encrypted Archive file.
- Insert the Passphrase used in encrypting the file
- Select ok to begin file extraction.

Alternatively, file from 7-zip application menu can also be selected by selecting the desired file to be extracted and clicking on the extract button from the menu. For further guidance and instruction, the help files by selecting help from the file menu then click on content.

B1 Free Archiver compared with other programs used for this study and commonly known encryption software, B1 free Archiver is large with an approximate file size of 44.55 MB. It is the second most compatible software with support for four common most used OS (windows, Linux, Mac Os and Android). It is also an Opens Source Application under the GNU LGPL license, which makes it accessibility span over both private and public usage. It supports 256bit AES Encryption Algorithm which according to [12] is still currently unbreakable except using brute force attack which is only easy and possible if password set is not strong enough. i.e using only small length numbers and alphabets with no capitalization and other characters as a password. After installing the software, the file size tripled to an approximate 140 MB which is due to offer special features like the file preview and beautified GUI offered by the software. It does not support self-extraction. For software developers and command line gigs B1 Free Archiver support command line interface which can be easily integrated into other software's for usability within the software's and also since it is an open source developer are free to lookup the source code to add, modify and make the application better and more suitable for the purpose they require it to perform. It integrates very well with windows operating system and provides easy access through the windows context menu. Below represents a graphical presentation of the software.

D. *Encrypting/Archiving File with B1 Free Archiver*

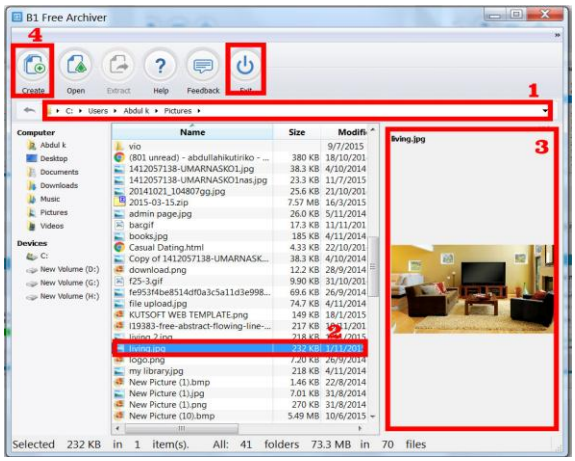

Figure 5. Encrypting/Archiving File with B1 Free Archive

Figure 5 depicts how B1 free Archive is used to create secured encrypted file after running the program.

- Address Bar shows the Address of the current working folder, if the need arises, easy navigation to the desired folder the files to be encrypted reside.
- Select file/Files intended to archive.
- This is a preview page used to preview your files, though, limited to only certain file types
- Create Button used to create the Encrypted file after the selection process.

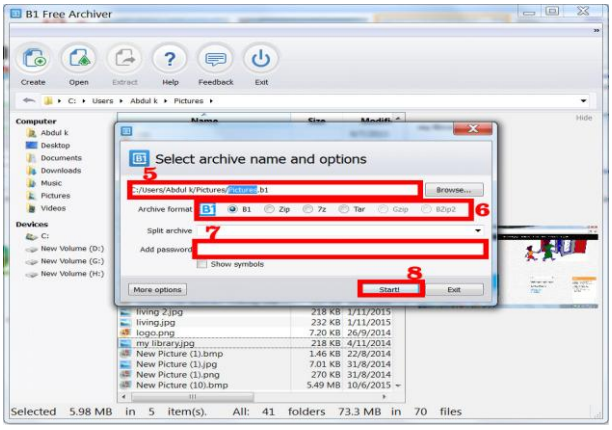

Figure 6. B1 Free Archive Encryption Menu

- This is where the location of the Output destination is set and also file name of the Encrypted file. By Default it is set to the destination of the selected file/files for Encryption and the name of the file if single or the name of the folder if multiple.
- This is the option used to select the type of archive to be created. by Default .B1 is selected which cannot be opened by any other known program

except B1 which provides it with another layer of security.

- This option allows you add Encryption to the Archive.
- After all, parameters are well inserted you then proceed by clicking this button to commit changes. If a password is inserted, a confirmation dialogue pops up to confirm the password and to prevent mistakes.

E. Extracting Files with B1 Free Archiver (Context Menu)

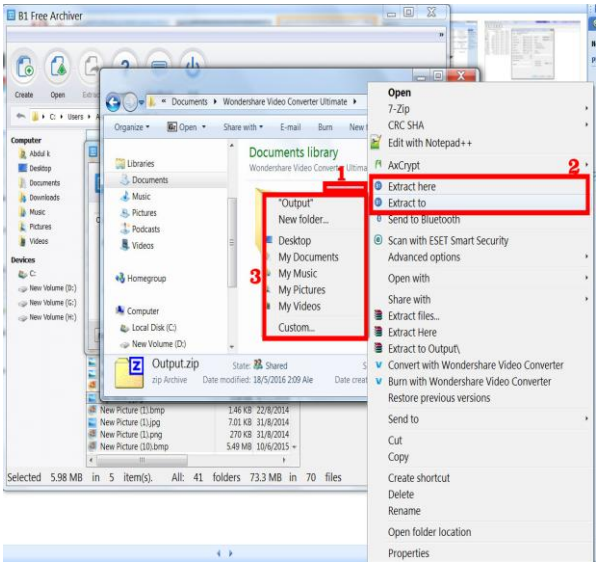

Figure 7. Extracting Files with B1 Free Archive (Context Menu)

The following are the procedure in extracting file from the context menu:

- Right-click on the desired file to be extracted.
- Select Extract Here from the context menu and the extracted files to be in the same Directory as the one are currently working on else are selected.
- Select "Extract to" for other options to populate describing where and how the downloaded files will be.
- A pop-up window appears asking to input the password used during the encryption before the extraction will begin.

B1 Free Archiver supports numerous archive file format and can be used for common Archive management alone that is (.B1, .zip, .gzip, others).

V. DISCUSSION

Nowadays information theft and ransomware are the leading threat to computer and digital data. It is believed that all cloud provider put in an extra effort to see that information stored with them are adequately secured and free from prying eyes. Although, that has not been able to totally prevent information theft and privacy intrusions. Some information gets into the wrong hands through malware installed on target computers [14], some through an insecure network and others through security breach on the cloud platform. Recently a collection of private pictures of various celebrities, mostly women and with many containing nudity were posted on the image board which was gotten from a hack on the cloud account of the celebrities, if the files were encrypted while uploading them, the hacker will have just been left with useless information since the main aim of encryption is to prevent unauthorized access. Also, there is a fear of administrators of the cloud accessing user information; this can be prevented using an encryption from the user end. AES 256 Encryption till date proves to be one of the best encryption algorithms with no known fact on crackability except using password guesses which can be prevented using stronger passwords.

7-zip is lightweight with little memory requirement and is compatible with most archive formats. It has a very high compression ratio with a simple to use user interface. B1 free Archive is very easy to use and with a very appealing graphical interface. It is simple flexible and supports numerous file extensions also with a B1 format that can only be extracted using the software itself.

When storing or would like to store your files in the cloud, make sure they are securely encrypted before uploading them to the cloud. Encrypting your files will safeguard the privacy of your data, which is especially important when storing sensitive corporate data or personal information that should never fall into the wrong hands.

VI. SUMMARY, CONCLUSION AND RECOMMENDATIONS

A. Summary

Encrypting files before been sent through any media or stored by the owner of the document is currently the best way of preventing unauthorized access to files. Cloud Computing offers enormous benefits to user in terms of file accessibility from any part of the world but has its limitations mostly in the area of Security. The most challenging obstacle to the acceptance of cloud is the security of data. Data is most valuable asset, individuals and organizations are really concern to know the status of their data. That is whether the data is safe or not.

When data are stored internally, individuals, companies, and government are rest assured of its security as they handle the overall control. Even though no warranty that data is more confined within when compared with the public cloud. The public cloud might be even more secured in storing data due to the fact that the providers of these services may implement advance level of security. Various methods of protecting data in the cloud have been implemented but full protection of data cannot be assured. Therefore the best way of securing files even on user's computer is by Encrypting sensitive information.

7-zip, B1 Free File Archive, and Axcrypt all provide secure encryption mechanism using AES 256-bit algorithm to effectively encrypt files. AES 256-bit algorithm currently has no proven record of crackability, which means any file encrypted with AES 256-bit is secure and cannot be accessed except by using the correct password set during encryption.

7zip support self-extraction this implies that a zip file can be created using 7zip that can extract itself without needing any zip manager or 7-zip been installed preinstalled on the system. It is the only one amongst them that support this feature. Some computer hardware vendors install 7zip on their machine during factory installation showcasing its wide acceptance and usability

B. Conclusion

Data encryption is very important nowadays due to increasing in data theft and independence on cloud platforms. The research work presents securing file on cloud computing system using encryption software: a comparative analysis.The encryption programs are 7zip, B1 free acrhiver and Axcrpt which are been compared on varieties of paramiters. The result have revealed that among the encryption softawares, 7zip work better due to its wide availability, light weight, faster encryption and better compression ratio when compared to the others.

C. Recommendations

File Encryption provides an efficient, secure, accurate, reliable way of securing sensitive information both on user computer and cloud. Companies and individuals should put in time and efforts to ensure that sensitive information is well encrypted to prevent unauthorized access. The following recommendations are proffered.

- Encrypting sensitive files and information before been uploaded to the cloud.
- Using a combination of alphabets, numbers and characters as Encryption password to reduce the possibility of brute force attack.

D. Suggestions for Further Study

- Design and implementation of encryption programs that is back to back compatible with all cloud service providers from the client's end.
- Implementing password strengthening parameters when setting up a password to ensure the user sees the strength of the password been set.

REFERENCES

[1] M. Maslin and R., Ailar "A Review of Cloud Computing Technology Solution for Healthcare System'. Journal *of Applied Sciences, engineering and technology* vol 8 iss.20, 2150-2153, 2014.

[2] K. Lakhtaria, "Next Generation Wireless Network Security and Privacy. Advances In Information Security, Privacy And Ethics.Retrieved from https://books.google.com.ng/books?isbn=146668688X and Accessed on 20th June, 2016.

[3] Priv, "Introduction to Cloud Computing". Retrieved from https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf, and Accessed 17th July 2016 and 2016

[4] A. Aized, M. Irfan, K. and A. Fazal, "Encryption techniques for cloud data confidentiality". International Journal of Grid Distribution Computing 7(4) 11 20 http://dx.doi.org/10.14257/ijgdc.2014.7.4.02 ISSN: 2005-4262 IJGDC 2014.

[5] M. Barry et al "A Brief History of the Internet.". Retrieved from www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet and accessed 17th July 2016 2009.

[6] R. O Ugwuoke, "Contributions and challenges of the internet to the development of university undergraduates" June 2013 retrieved from google and accessed on 27/07/2016

[7] Cyber Centre, "Cloud Computing Security Considerations" updated 2012, 2011.

[8] R. Tim, "Five things you should know about cloud security". Retrieved from https://blogs.microsoft.com/cybertrust/2016/01/06/five-things-you-should-know-about-cloud-security and accessed on 17th July 2016.

[9] G. Eugene, "Cloud Computing Models**"** Composite Information Systems Laboratory (CISL), Sloan School of Management, Room E62-422, Massachusetts Institute of Technology. 2013

[10] A. Huth and J. Cebula "The Basics of Cloud Computing". Retrieved from https://www.uscert.gov/sites/default/files/.../CloudComputingHuthCebulaand accessed 17th July 2016 2011.

[11] A. W. Khan, S. U., Khan, M. Ilyas and M. I. Azeem, "A literature survey on data privacy/protection issues and challenges in cloud computing". IOSRJCE, vol 11 pg., 28-36, 2012.

[12] M. Swapnali and C. Sangita. "Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization retrieved from www.sciencedirect.com accessed on 20th August, 2016, 2016

[13] B.Subramani and P.N.Indu Vikashini "A security issues on cloud com puting" worldwidejournals.com/paripex/file.php?val=April_2016_1460809682__130..2016

[14] N. Dave, "AES encryption is cracked Researchers find a weakness in the algorithm". Retrieved from http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked. 2011and accessed 17th January 2016.

[15] C., Sneha, C. A. Suriya, and S. Indhumathi, "A secure the data in cloud by using private auditing scheme". Retrieved from http://www.ripublication.com and accessed on 20th august 2016, 2016

[16] A. J. Emily and S. Karthigaiveni, "New Public Integrity Auditing Scheme for Cloud Data Storage Using Mac And Symmetric Key Cryptographic Algorithms". International Journal of Applied Engineering Research vol. 11 issue 3, pp 1894-1899 retrieved from http://www.ripublication.com and accessed on 20th august 2016

[17] T. Gaur and D. Sharma, "A Secure and Efficient Client-Side Encryption Scheme in Cloud Computing." I.J. Wireless and Microwave Technologies, vol 1, 23-33 Published Online January 2016

[18] M. Priyanka and S. Priya, "Cloud Data Outsourcing and off sourcing using trust computation" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 iss.3 , 2016, 1417-1424, 2016.

[19] S.V. Tikore and D. K Pradeep, "Ensuring the Data Integrity and Confidentiality in Cloud Storage Using Hash Function and TPA". International Journal on Recent and Innovation Trends in Computing and Communication.Vol.3 Iss. 5, 2015

[20] S. Yogesh and V. Alka, "Privacy Preserving using Data Partitioning Technique for Secure Cloud Storage" International Journal of Computer Applications (0975 – 8887) vol. issue 116 (16). Retrieved from research.ijcaonline.org/volume116/number16/pxc3902721.pd access on 20th march 2016

[21] D Rani and R. K. Rajan, "Enhance data security of private cloud using encryption scheme with RBAC". International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014

[22] A. Dharini, et al "Data Security for Cloud Computing Using RSA with Magic Square Algorithm". International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 11 No. 2 2014, pp. 439-444.