International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-3 Issue-16 September-2014

Performance Analysis of Client Side Encryption Tools

Subrata Kumar Das[1], Md. Alam Hossain[2], Md. Arifuzzaman Sardar[3], Ramen Kumar Biswas[4], Prolath Dev Nath[5]

Abstract

Client side encryption tools are becoming popular among cloud users to increase the security of their data stored in the cloud server. Several client side encryption tools have been already introduced with their own features and security schemes. It is necessary for users to find out the best tool for encrypting data and storing it in the cloud. "Which one provides more security from those tools? Which one consumes less time? In a word, which one is the best?" These are the open questions to the users, now-a-days. To find out the best tool, we have analyzed the performance of the selected tools namely Boxcryptor, Ensafer, SharedSafe, SafeMonk and Cloudfogger. To measure the performance, we have calculated the upload time (encryption and synchronization time) for different sizes of data for each tool. Comparing the performance among these tools, we have obtained the best tool.

Keywords

Cloud Computing, Encryption tools, CSPs, Security.

1. Introduction

Cloud computing is a well known matter now-a-days. It is a computing service through the cloud in a real time communication (internet), where cloud is a set of hardware, storages, networks, applications and interfaces. Important files can be stored in the cloud through different cloud service providers such as SkyDrive, Dropbox, CloudMe, Google Drive etc. Since, the data passes through the internet and stored in a remote server so, the hackers can easily access those data. It is very necessary to ensure the security so that no one can access our valuable data. With the help of encryption technique, we can ensure the security of these files.

Encryption is the process of converting data into another form known as ciphertext and without authorization, nobody can access it. The client side encryption tools are mainly used for encrypting our important files and uploading the encrypted files in the cloud. Now-a-days, various client side encryption tools are available in market such as Boxcryptor, Ensafer, Cloudfogger, SharedSafe, SafeMonk etc. For user convenience, they need to know which tool has the best efficiency and ensure best security? Moreover, which tool should they use? For this reason, we select the most popular five client side encryption tools namely Boxcryptor, Ensafer, Cloudfogger, SharedSafe and SafeMonk to analyze their performances and compare the performances. In this way, we can find the best client side encryption tool.

2. Cloud Service Providers (CSPs)

By using private and public cloud, service providers provide software services. It means that the storage and software is available and we can access it through the internet [1]. Cloud services are mainly designed to provide easy, scalable access to applications and services which are maintained by a cloud services provider [2]. The service provider provides software and hardware and it is essential for the service because dynamically cloud service may be able to fulfil the purpose of its user. With the help of cloud service, we can easily store our valuable data with backup solution.

A company that provides some features of cloud computing based on their services which include Infrastructure as a Service (IaaS) using virtual servers and virtual storage, Software as a Service (SaaS)

Manuscript received September 18, 2014.

Subrata Kumar Das, Department of Computer Science and Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

Md. Alam Hossain, Department of Computer Science and Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

Md. Arifuzzaman Sardar, Department of Computer Science and Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

Ramen Kumar Biswas, Department of Computer Science and Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

Prolath Dev Nath, Department of Computer Science and Engineering, Jessore University of Science and Technology, Jessore-7408, Bangladesh.

which indicates conversion of simple software to complex via the internet and Platform as a Service (PaaS) that indicates both IaaS and SaaS and its output is called unified service is known as cloud provider. It is often known as cloud service providers or CSPs [3].

Cloud providers deliver their cloud solutions depending on the users demand. Cloud provider means public cloud provider, private cloud provider, and hybrid cloud provider.

Google Drive, Dropbox and SkyDrive are the most commonly used cloud service providers.
Dropbox: Dropbox is a personal cloud storage that is privately used and files hosting service also known as online backup service. It is frequently used for file sharing and collaboration. The operating system Windows, Macintosh and Linux are supported by it [4]. Dropbox ensure the facilities for Android, iPhone and BlackBerry. Here, user data is protected with Secure Sockets Layer (SSL) using Advanced Encryption System (AES) 256-bit encryption.
SkyDrive: SkyDrive is personal cloud storage service and file hosting services from Microsoft. Using the tool users can upload and synchronize files to cloud storage. Users access their data from web browser [5], [6]. By using SkyDrive, any user keeps their files privately but shares their data publicly. Windows and MAC as well as mobile devices like Smartphone's and tablets, including Windows phone 7 and 8 devices, Apple iOS powered iPhones and iPads are supported by it.
Google Drive: Google Drive is also personal cloud storage which is a premium cloud storage service from Google that helps users to store and synchronize digital content information and computers, laptops and some mobile devices such as Android, Apple iOS-powered iPhones and iPads touches [7]. The operating system Windows, Android and iOS are supported by it.

3. Methodology

The problem can be stated in short as: now-a-days, we have different client side encryption tools with different features (encryption technique, cross platform, file sharing etc). It is necessary to find out the best client side encryption tool among the existing tools in terms of user requirements. The best client side encryption tool could be found in different ways as their encryption speed, uploading speed, key length and file sharing technique and they differ from each other. In this paper, we measured the efficiency of different tools using performance of encrypting data and uploading the encrypted data in the cloud to find out the best client side encryption tool.

We compared the performances (uploading time= encryption time + synchronization time) of five client side encryption tools which are available in the market namely Boxcryptor, Ensafer, SharedSafe, SafeMonk and Cloudfogger. Here, encryption time is the time taken by a tool for encrypting a file completely, where file is an object that stores information, data in a computer system. Storing the encrypted file in the cloud service provider's folder in our system, it takes some time for synchronizing with the cloud server. This time is known as synchronization time. We took various sizes of file (like 256KB, 512KB, 1024KB, 3072KB and 5120KB), encrypted them with these tools and stored them in a cloud service provider (Dropbox). The total uploading time for an individual tool is measured manually (with the help of a Stopwatch). Comparison among their performances, we found the best client side encryption tool.

4. Deriving the attributes of existing Tools

A. Boxcryptor

Boxcryptor protects the clients file securely in a cloud. It has a file key, user keys, password key, group key and company keys [8]. To encrypt and decrypt a file, AES encryption key is used in the file key. In the user keys, every user has a RSA key pair (private and public) and an additional AES key. By using password, we can get AES encryption key with the help of key strengthening and stretching function PBKDF2 with HMACSHA512, 10.000 iterations and a 24 byte salt. In the group key like as users, every group consists of RSA key pair and an additional AES key. Every group is also identified by its unique key, the company key also like as user's keys and it has RSA key pair (private and public) and an additional AES key. It supports both file and filename encryption manually and automatic transparent. It has also sharing access system to a file or folder. Information can be stored in the Boxcryptor after creating virtual drive and that information will be automatically encrypted. It works with Dropbox, SkyDrive and other cloud drive services [9].

Users often keep physical control over their user information and keys. It can be done by using

Boxcryptor with a local account instead of a Boxcryptor account that is stored at the Boxcryptor key server [8]. With the help of local account, all user information and key data are stored in a key file on the local device and they never transfer to the Boxcryptor key server. Local accounts can easily be converted to Boxcryptor accounts at any time. The users will have to ensure a password, when they encrypt a folder with Boxcryptor [9]. Strong password includes mix letters, numbers and other symbols. For backup, they need to save a configuration key file. The configuration key file is used if any fault happens in users machine and they need to recover the files from backup from a new machine. It should be noted that if users want to hide files from Dropbox, use the defaults configuration. Without configuring mount drive for remembering the password, any user can hide their files from others. The operating system Windows, MAC, iPhone, iPad and Android are supported by it [10].

B. Cloudfogger

Cloudfogger is simple to design and secured by using AES encryption algorithm for transparent encryption. Cloudfogger can be used free for file encryption on the computer, mobile devices. After encrypting all the files, they are uploaded to the cloud [11], [12]. It ensures that Dropbox and any others services never get permission to access the files. Dropbox, SkyDrive, Google Drive or any other cloud storage service can be integrated with it. The operating system Windows, MAC, OSX and Android are supported by Cloudfogger and iPad, iPhone are on the way.

The encryption algorithms of Cloudfogger include [13]:

1. By using AES 256bit in OFB mode and a 4KB block size, data is stream encrypted easily.
2. A unique AES key is used for every file.
3. AES keys are secured with user's RSA public key and the user cannot access the AES key and data without the private key.
4. If multiple users need to access a file, then AES key is included in multiple headers within the .cfog-file, each RSA is protected for corresponding user.

The server is used to store the encrypted keys except the password as well as users hard disk. So, anybody will never get access to RSA key in case of a lost password without password recovery turned on [13].

After password recovery option activated, the password hash gets stored on the Cloudfogger servers otherwise, failed to store it. To recover a lost password, user need a verification mail which is sent to the owner of the account. The verification code given in this mail is used to continue with the password recovery. In case of changing password in the Cloudfogger setting, the password recovery turns on or off. A physical layer exists between the encryption service and the storage location of data, if data is encrypted on the client side and stored at cloud storage service. The encrypted file that exists in the folder is seen by the cloud. When anyone signed to Cloudfogger, then these files are displayed locally as decrypted files [12]. In Cloudfogger, it is easily possible to access the files without internet access. If anyone is not able to access the Cloudfogger servers (there is no internet access with the devices), then it will still possible to decrypt the encrypted data with Cloudfogger. The only requirement in this case is that he/she has successfully logged in once in Cloudfogger on this device and it is an important advantage for Cloudfogger.

Cloudfogger is free encryption software and it counts only security. Cloudfogger is based on the following principles:

1. It provides robust, industry-standard encryption with absolutely proven encryption algorithms.
2. Without the correct password, no one can be permitted to decrypt files.

Without providing the Cloudfogger identity, users can easily share encrypted files with others. This allows as secure usage of shared Dropbox folder.

C. Ensafer

Ensafer is used as client side encryption tool. It gives service same as Boxcryptor. Ensafer is a multilayered integrated end system security solution which provides confidentiality, integrity, authentication, application and user transparency, central administration console for policy formulation and enforcement and network access control [14], [15]. For the TCP and UDP application, it provides security and it is simple to design. So, Ensafer provides several options that include encryption, secure collaboration, secure Storage and secure file sharing. The salient features which are essential for the Ensafer [14], [15], [16] are given below:

1. It provides end-to-end security system and their communication.
2. It has application transparency that includes exchange of session wise key and encrypted communication.
3. It is based on three level authentications that include user authentication, network packet's

authentication and machine authentication based on its signature.
4. It includes integrity of TCP based network communication option.
5. It provides unique technique mechanism that is used for machine authentication which is based on machine fingerprint generated from various system parameters.
6. It provides role based network access control system and multi-layered defense option.
7. It has plug in support system which is used for crypto algorithms and user authentication modules run on Windows and Linux.

Ensafer has two types of component, namely client component and server component [15]. Client component includes security policy enforcement agent and application that need to be installed on secured system. The Server components are administration console GUI, client and user database. Ensafer supports all major hosting and sharing services such as Google Drive, Dropbox, SkyDrive etc [17]. The operating system Windows and Linux are supported by it. By using Dropbox and Ensafer users can easily share a folder to other and only the private key of Dropbox user can decrypt this folder. In the folder the files can be read and decrypted by Dropbox user rather than others. After installing Ensafer on computer, users can get access to encrypted data. Here all encryption and synchronization happens automatically.

D. SafeMonk

SafeMonk is one of the client side encryption tools. It solves the large problems with the help of Dropbox security in order to protect ones sensitive files. The operating system such as Windows XP and 7, MAC, Windows 8, iPhone and iPad and Android are supported by SafeMonk except Linux [18]. SafeMonk has key generation and random number generation. In the key generation, server never generates the encryption keys because client side can be used to perform the key generation. The keys are generated only when users create an account and install the software. The security system of SafeMonk is provided by AES-256 and RSA. It provides a hostproof solution for Dropbox which consists of encryption and key management algorithms [19], [20]. This indicates that someones service and data is stored on his networks and those are not capable of discovering others keys. Dropbox data is secure from decryption as long as user uses this system. The loss of data from the servers happens if the server attacks and never gives any result in the exposure of any sensitive key component that could be used to decrypt data. SafeMonk folder exists with other folder under Dropbox account. Any document remaining in this folder is secured. SafeMonk encrypts the data quickly and Dropbox may be able to start the synching content [18]. That means if anybody want to use SafeMonk, then he/she must have to install it on all devices and machines and it create a SafeMonk folder inside Dropbox. Anything remaining in SafeMonk folder will be encrypted and Dropbox will synch that encrypted files. The SafeMonk provides tapproof solution system which means only user can access their file [18]. So, SafeMonk is a tapproof encryption system for sensitive data in Dropbox. If we share a folder with someone, then he can only see the folders that we shared and not to do anything without keys. SafeMonk supports only secure folder sharing rather than individual file sharing.

In case of sharing in the SafeMonk, it provides least sensitive key for supporting the share. Moreover, currently folder based sharing delivers the DEK (Directory Encryption Key) of that folder, thus allowing unlocking of everything underneath [19]. The FEK can be used for supporting the shared files that includes:
1. KEK (Key encrypting Key): Most sensitive key which is used to unlock everything.
2. FEK (File Encryption Key): Less sensitive key.

In a SafeMonk, after creating a password for the user account, the client creates a hash for the corresponding password and the hash is not stored anywhere except SafeMonk server [19]. The hash of the password is used to authenticate the server. Hash value never gives the corresponding password.

E. SharedSafe

In order to use SharedSafe, we do not need sign up because SharedSafe is file synchronization and sharing application [21]. SharedSafe supports online storage like as Dropbox.
The storage system is safe here as SharedSafe’s encryption is known as open source. SharedSafe encrypts the data and names of files and store file in safe with the help of encrypted file system. MAC and Windows operating system are supported by SharedSafe and Linux is on the way. The export key is supported by SharedSafe and without this key and internet connection nobody can access the files.

Exported safe contain very sensitive information that includes [21]:
1. The login identity of the email account where the safe resides in.
2. To read and write the file system tree in the safe, we need encryption key.

SharedSafe never supports any automatic distribution of safe keys because it manually distributes safe keys as users need and supports the safe key with import files from and exports them to local files on their computer. Users also have private keys for its safe key encryption and are able to decrypt all the safe keys that are created by SharedSafe and safe keys are very sensitive objects. The security system of SharedSafe is determined by AES. When all local folders are linked together in our computer to safe, then SharedSafe synchronizes the files automatically and it's linked safe that is known as linked folder [22]. If we want to change safe file or modify, then we have shared the safe and it is synchronized back to its linked folder and SharedSafe will keep a copy of them in recycle bin. We can also work with those file without internet connection. SharedSafe also run behind firewall [21]. SharedSafe connects safe by using either FTP or IMAP protocol and FTP and SharedSafe use firewall in passive mode connect to server.

F. Comparison table of Existing Tools

After analyzing the existing tools, we have found some similarities(encryption, decryption, sharing etc.) and dissimilarities represented in table 1.
We can easily notice that almost all the tools use AES and RSA algorithms for encryption and key generation. All the tools except SharedSafe have authentication feature. Without this authentication, no encryption or decryption is possible in those tools. Almost all the tools support Dropbox as CSP and some tools also support other CSPs such as SkyDrive, Google Drive etc. All the tools support Windows OS and some of them support MAC, iOS, Android etc. In case of sharing, Boxcryptor, Ensafer and Cloudfogger support all kinds of sharing (both file and folder). SharedSafe supports folder sharing only. Cloudfogger, Ensafer and SafeMonk support offline encryption and decryption and once it is authenticated for the first time in a device.

SharedSafe performs offline encryption to a linked safe and can be accessed over internet by using safekey from the recipient end. Among these tools, only SharedSafe can create safe key in offline. Boxcryptor supports encryption and decryption even though the device is currently offline after a successful logged in until the system shutdown. The comparison table of client side encryption tools is given below:

Table 1: Comparison table of exiting tools

Parameter	Boxcryptor	Ensafer	SharedSafe	SafeMonk	Cloudfogger
Used encryption algorithm	AES, RSA	AES, RSA	AES	AES-256, RSA	AES-256,RSA
Supported providers	Dropbox, MS SkyDrive, SugarSync, Box, One Drive	Dropbox	Dropbox, email storage Services	Dropbox	Dropbox, SkyDrive, Google Drive
Supported platforms	Windows**,** MAC**,** iOS, Android, Blackberry 10 and Google Chrome	Windows, Linux	Windows, MAC	Windows, MAC, iOS and Android	Windows, MAC, iOS and Android
Sharing	Secure file Sharing, support for mobile Apps	File or folder sharing	Folder sharing	Secure sharing, remote wipe, account recovery	File sharing, portable file format, file distribution via email
Authentication required	Yes	Yes	No	Yes	Yes
Offline encryption	Yes	No	Yes	No	Yes

G. Issues and challenges of existing tools

In this section, challenges for the existing client side encryption tools are highlighted.

Advantages of Boxcryptor:
1. It is secured because its security system constructed with AES and RSA algorithm.
2. It supports file and filename encryption both manualy and automatic.
3. It supports cross platform (Windows, MAC, OSX and Android).
4. Encryption and decryption takes place directly on device i.e. password never transfers to anywhere.

5. Available for all major cloud storage providers (Dropbox, CloudMe, Google Drive, CloudSafe etc).

Disadvantages of Boxcryptor:
1. Since, encryption needs more storage than the unencrypted files that’s why a 2 GB file need to waste 4 GB+ space of our HDD, when we put it in the mount drive.
2. We cannot add any sub folder that already indicates existing location.

Advantages of Cloudfogger:
1. It works with the SkyDrive, Dropbox, Google Drive and Box.
2. It removes waste space problem of Boxcryptor by using on the fly system for encrypting file directly.
3. The operating system Windows, MAC, OSX and Android are supported by Cloudfogger.
4. AES keys are protected with user's RSA public key and the user with the private key can access the AES key and thus the data.

Disadvantages of Cloudfogger:
1. Syncing function is not automated so, users have to manually download and upload files.
2. iPhone and iPad are not supported by it.
3. If we lost password, then we cannot access the stored data without password recovery turned on.

Advantages of Ensafer:
1. Files can be placed anytime in the Ensafer physical directory without logging in to the server. That is, Ensafer folder can be used to store files without Ensafer and Dropbox running.
2. It provides end to end encryption technology which is very strong to encrypt in cloud service like Dropbox.
3. Ensafer security component is determined by AES and RES end to end encryption.
4. Ensafer is a multilayered integrated end system security that provides confidentiality, integrity, authentication, application and user transparency.
5. Anybody can easily delete, download and upload files again and again to make our Dropbox secure.

Disadvantages of Ensafer:
1. It is difficult to store and share data on the internet with the help of this tool.
2. It does not give enough security about sensitive information.
3. It has no application on mobile yet.

Advantages of SharedSafe:
1. SharedSafe supports online storage (memory) and turns email accounts into online file storage.
2. In order to use sharedsafe, we do not need sign up because SharedSafe is file synchronization and sharing application.
3. SharedSafe encrypts names and data of the file and store file in safe with the help of encrypted file system.
4. It has also been designed for maximum transfer.

Disadvantages of SharedSafe:
1.Linux is not supported by it.
2.SharedSafe does not support any automatic distribution of safe keys.
3.Rather than individual file data, the whole file is encrypted.

Advantages of SafeMonk:
1. It solves the large problems by using the Dropbox security in order to protect sensitive files.
2. Windows XP and 7, MAC, windows 8, iPhone and iPad, Android are supported by SafeMonk.
3. It is known as hostproof that means it cannot notice user’s files.
4. SafeMonk is known as tapproof that indicates nobody gets permission to access files except user’s approval.
5. If passwords are lost, SafeMonk offers account recovery via a one-time recovery key.

Disadvantages of SafeMonk:
1. The operating system Linux is not supported by it.
2. SafeMonk only delivers the least sensitive key required to support the share.
3. SafeMonk servers never store the recovery code.
As seen above, the issues and challenges of the existing tools are listed. In the next section, performance analyses of the selected tools are described.

5. Performance analysis and results

In this section, the selected client side encryption tools namely Boxcryptor, Ensafer, SharedSafe, SafeMonk and Cloudfogger are analyzed and their issues and challenges were explained.

A. System Setup

In this section, the application tools which are necessary for selecting the best client side encryption tool will be examined. Further, the testing environment is described.

a. Application Tools

The application tools used for the analysis are listed below:

1. Boxcryptor
2. Ensafer
3. SharedSafe
4. SafeMonk
5. Cloudfogger

These are the client side encryption tools which were installed in the testing environment.

6. Dropbox

This application tool is used as a cloud service provider for storing the encrypted data.

b. Testing Environment

Same machine was used for all the experiments shown in the further sections.
The specifications of the computer used are:

1. Operating System - Windows 7.
2. Processor – Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz.
3. RAM - 4GB (DDR-3).
4. Clock - core speed 3093.0 MHz, bus speed 99.8 MHz.
5. Main Board – Intel (Model - DH61WW).
6. Bandwidth – 1 mbps.
7. Stopwatch.

B. Analysis

The performance of each selected tool is described with corresponding table and performance graph. At the initial stage, we installed each tool and with the help of these tools, different sizes of data were encrypted and uploaded. We used a stopwatch to read the upload time for each individual size of data for three times and counted average time as showen in below for each individual data. Finally, we obtained the average upload time from average time of different sizes of data. The performance graph was obtained by plotting the value of data size (KB) in the Y axis and the upload time (sec) in the X axis.

After installing the Boxcryptor, Cloudfogger, Ensafer, SafeMonk, and SharedSafe, we took 256KB, 512KB, 1024KB, 3072KB and 5120kB sizes of data for encrypting and uploading them in Dropbox. Then we got different upload time in different tools.

a. Performance of Boxcryptor

The average upload time of Boxcryptor is 55.602 sec is shown in table 2.

Table 2: Performance table of Boxcryptor

Tool	Data size (KB)	Upload Time (second)				Average Data size (KB)	Average Upload Time (second)
		1st step	2nd step	3rd step	Average		
Boxcryptor	256	10.3	12.7	11.9	11.63	1996.8	55.602
	512	22.3	23.14	21.4	22.28		
	1024	35.6	37.0	34.9	35.83		
	3072	87.0	84.0	89.0	86.67		
	5120	121.0	121.6	122.2	121.6		

Performance of Boxcryptor with graphical representation is given below:

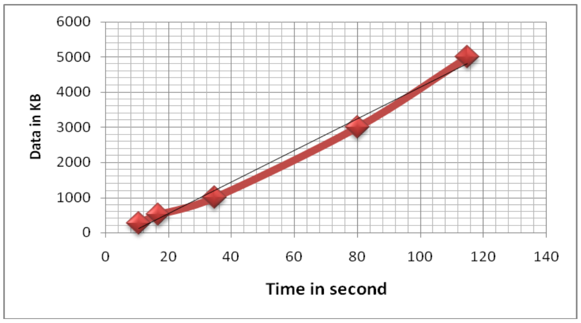

Figure 1: Graphical representation of the performance of Boxcryptor

b. Performance of Cloudfogger

The average upload time of Cloudfogger is 51.354 sec is shown table 3.

Table 3: Performance table of Cloudfogger

Tool	Data size (KB)	Upload Time (second)				Average Data size (KB)	Average Upload Time (second)
		1st step	2nd step	3rd step	Average		
Cloudfogger	256	10.4	10.6	10.3	10.43	1996.8	51.354
	512	17.0	16.8	16.5	16.77		
	1024	34.1	34.6	35.0	34.57		
	3072	80.0	82.0	78.0	80.0		
	5120	110.0	115.0	120.0	115.0		

A graphical representation of the performance of Cloudfogger is given below:

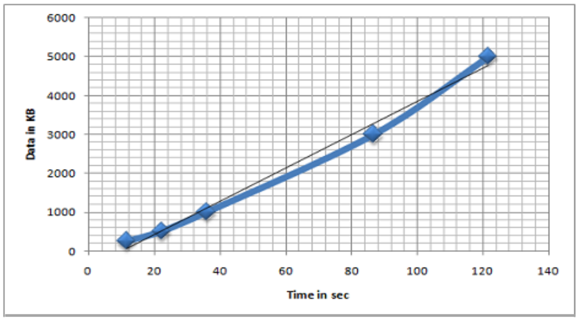

Figure 2: Graphical representation of the performance of Cloudfogger

c. Performance of Ensafer

We took 256KB, 512KB, 1024KB, 3072KB and 5120KB sizes of data for encrypting and uploading the encrypted copy in Dropbox with the help of Ensafer (after installing the EnSafer) as shown in table 4. The average upload time is 53.312 sec (from table 4).

Table 4: Performance table of Ensafer

Tool	Data size (KB)	Upload Time (second)				Average Data size (KB)	Average Upload Time (second)
		1st step	2nd step	3rd step	Average		
Ensafer	256	12.5	10.5	10.8	11.26	1996.8	53.312
	512	18.7	17.0	16.5	17.4		
	1024	33.9	34.1	35.6	34.53		
	3072	81.0	78.0	83.0	80.67		
	5120	123.0	124.0	121.2	122.73		

The performance graph of Ensafer is given below:

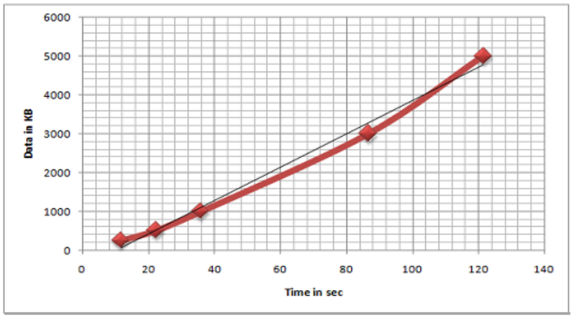

Figure 3: Graphical representation of the performance of Ensafer

d. Performance of SafeMonk

Here, 256KB, 512KB, 1024KB, 3072KB and 5120KB sizes of data are taken by the SafeMonk for encrypting and uploading data in Dropbox and measuring the average upload time. The average upload time of SafeMonk is 52.34 sec (from table 5).

Table 5: Performance table of SafeMonk

Tool	Data size (KB)	Upload Time (second)				Average Data size (KB)	Average Upload Time (second)
		1st step	2nd step	3rd step	Average		
SafeMonk	256	10.8	10.4	10.4	10.54	1996.8	52.34
	512	18.6	16.5	16.6	17.23		
	1024	34.5	34.1	34.6	34.4		
	3072	80.0	76.0	78.0	78.0		
	5120	119.0	123.6	122.0	121.53		

The performance graph of SafeMonk is given below:

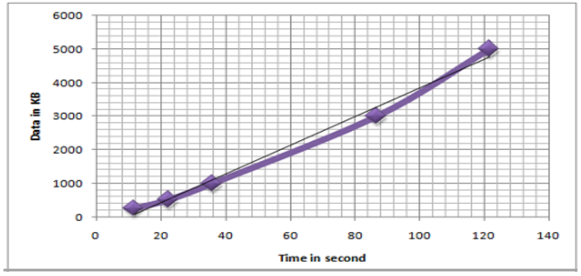

Fig. 4: Graphical representation of the performance of SafeMonk

e. Performance of SharedSafe

Various sizes of data like 256KB, 512KB, 1024KB, 3072KB and 5120KB are taken by the SharedSafe for measuring the average upload time after encrypting and uploading data in Dropbox. The average upload time of SafeMonk is 52.324 sec (from table 6).

Table 6: Performance table of SharedSafe

Tool	Data size (KB)	Upload Time (second)				Average Data size (KB)	Average Upload Time (second)
		1st step	2nd step	3rd step	Average		
SharedSafe	256	10.4	10.8	10.7	10.63	1996.8	52.324
	512	17.9	16.5	16.8	17.06		
	1024	34.5	34.1	34.6	34.4		
	3072	80.0	76.0	78.0	78.0		
	5120	119.0	123.6	122.0	121.53		

The performance graph of SharedSafe is given below:

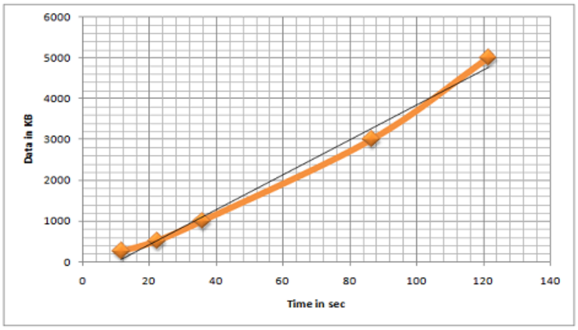

Figure 5: Graphical representation of the performance of SharedSafe

Now, the performances of all these tools are given in a graph. Here the y axis represents the upload time in seconds and x axis represents data size in KB.

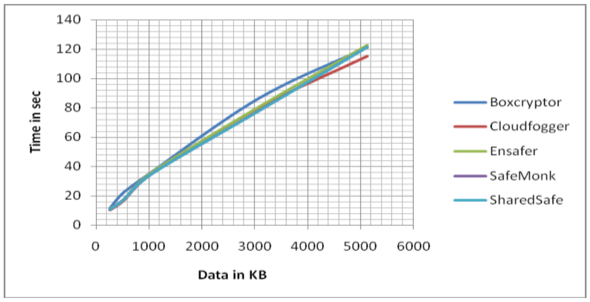

Figure 6: Graphical representation of the performance of all tools

C. Results

From the table 2, 3, 4, 5 and 6, we get the average upload times of five different client side encryption tools. Using these reading, we can detect the best tool among these tools by comparing the values (average upload time).

Table 7: Average uploads time of these tools

Tools name	Average Data Size	Average Upload Time
1. SharedSafe	1996.8 KB	52.324 seconds
2. Boxcryptor		55.602 seconds
3. Cloudfogger		51.354 seconds
4. Ensafer		53.312 seconds
5. SafeMonk		52.34 seconds

The graphical representation of the average uploads time of different tools for comparison is given below:

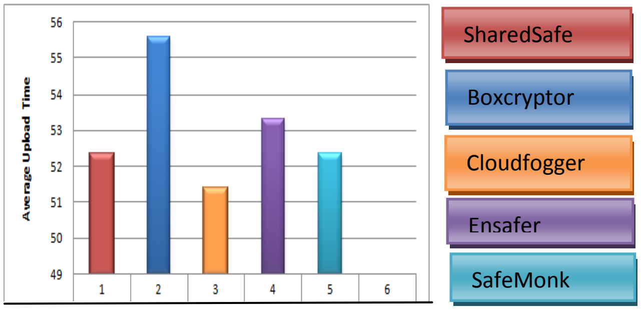

Figure 7: Graphical Representation of average upload times of different tools.

Now, if we compare the average upload times, we can say that Cloudfogger has the minimum average upload time than the other tools. So, Cloudfogger is the best client side encryption tool.

6. Conclusion

In cloud computing, client side encryption tools play a very important role for the security of important files stored in the cloud. In this paper, we have find out the best client side encryption tool from five available tools by comparing their performances (best tool selected based on upload time). Deriving attributes of the selected tools and their issue and challenges were given in this paper.

Performance analysis of the selected tools was also described above. In section V, the performance of each tool was calculated and compared with each other. After analyzing and comparing the performances, we have found Cloudfogger as the best client side encryption tool.

References

[1] http://www.webopedia.com/TERM/C/cloud_provider.html.
[2] http://www.webopedia.com/TERM/C/cloud_services.html.
[3] http://searchcloudprovider.techtarget.com/definition/cloud-provider.
[4] http://searchconsumerization.techtarget.com/definition/Dropbox.
[5] http://www.webopedia.com/TERM/S/skydrive.html.
[6] http://en.wikipedia.org/wiki/OneDrive.
[7] http://www.webopedia.com/TERM/G/google_drive.html.
[8] https://www.boxcryptor.com/en/technical-overview.
[9] http://jameswharris.wordpress.com/2013/02/03/dropbox-and-boxcryptor-the-dangers-of-encrypting-your-digital-life/.
[10] http://networkedblogs.com/FUpXF.
[11] http://www.cloudfogger.com/en/.
[12] http://networkedblogs.com/FUpXF.
[13] http://support.cloudfogger.com/index.php?/Knowledgebase/Article/View/13/7/what-type-of-encryption-does-cloudfogger-use.
[14] http://cdachyd.in/products/ensafe-1/Ensafe.pdf.
[15] http://www.cdactvm.in/images/Track2/Session2/END%20SYSTEM%20SURAKSHA%20FRAMEWORK%20(ENSAFE).pdf.
[16] http://pune.cdac.in/html/events/hyd/ensafe.aspx.
[17] http://www.crunchbase.com/company/ensafer.
[18] https://www.safemonk.com/faq.
[19] http://support.safemonk.com/customer/portal/articles/976926-safemonk-security-overview-and-definition
[20] https://www.safemonk.com/security.
[21] https://www.sharedsafe.com/faq/.
[22] https://www.sharedsafe.com/how-it-works/.

Subrata Kumar Das was born in Narail, Bangladesh, in 1980. He received the B.Sc. and M. Sc. degree in Computer Science and Engineering from the Islamic University, Kushtia, Bangladesh, in 2004 and 2005 respectively.

In 2009, he joined as a Lecturer in the Department of Computer Science and Engineering of Jessore University of Science and Technology, Jessore, Bangladesh. Since 2012, he has been with the Department of Computer Science and Engineering, Jessore University of Science and Technology, Jessore, Bangladesh, as an Assistant Professor. His research interest on the field of Cloud Computing, Parallel and Distributed Systems, High-performance and Low-Power Real-Time Systems, Mobile Embedded Systems and Network Security.