A SURVEY: CLOUD BASED STORAGE SECURITY "DROPBOX"

Waleed T. Al-Sit
Department of Computer Engineering.Mu'tah University. Al-Karak, Jordan.
w_sitt@hotmail.com

ABSTRACT*: Cloud computing is being used a lot these days, it supports dynamic scalability via using virtual resources, and they serve many applications. Many cloud service providers offer these services for free. There are several classifications according to the service provided by cloud services; one of the popular classifications is collaborative cloud services such as Dropbox. Dropbox is a data storage service which is implemented as a synchronization service like apple cloud application, Google storage application and Amazon S3 application for online storage. Dropbox cloud storage service is an easy and suitable way of storing files and accessing them, using the internet, these stored files are distributed among the internet to do some computation or to store them. Dropbox provides reliable file storage in addition to files synchronization and user collaboration, but the delay of the synchronization of the Dropbox users increases while expansion. n order to keep the cloud white we must ensure that the files are secured and the service is available, and also the client cannot get attacked by different attackers. On this topic, many methods have been developed in order to avoid attacker and to keep such applications secured.*

Keywords— Cloud computing; Dropbox; Amazon; virtual resources;

I. INTRODUCTION .

Cloud storage is a network system that store data in virtual spaces which are managed and hosted by other parties that have large data centers those data centers save the users' data for an amount of money or for free as the application needs [4.]. Dropbox is one of the most popular cloud storage applications that was created in 2007 by Drew Houston and Arash Ferdosi, tow MIT students were tired from Sending emails to themselves to work from multiple computers [5]. Since 2007, Dropbox has been the most popular online storage service that can be used in many types of communication devices such as mobiles, computers and online web pages.. It's used for uploading and downloading files and folders such as images, videos, files or any type of data that can be stored. Dropbox is one place for your staff at any time and anywhere among the network. At any time you can drop your data and they will automatically show up on your computers, phones and also on the Dropbox website and you can access Dropbox from anywhere [5].

Recently, the Dropbox website announced that there are 275 million of users using Dropbox in April 2014 while it had 200 million of users in November 2013 and this is a noticed increase in the number of users of Dropbox [11]. More than 100 billion files are being stored by users and 1 million files are being saved every 5 minutes [7]. Dropbox accounts about 100 GB which is equivalent to 4% of the total traffic on some monitored networks the rest of the traffic was mostly on YouTube these results were taken from monitoring 42 consecutive days by some researchers. These results were taken from monitoring the traffic on two university campuses and points of presence (POP) in a large internet service provider (ISP). The ability to share content is the main feature in Dropbox and as some researches, 30% of home users have many devices that are linked with each other, and 70% of them share at least one folder [6].

In this paper, I will firstly mention the Dropbox features as a distributed system and explain each feature alone. Section 3 includes an explanation of the Dropbox design with important detailed information. Section 4 concludes this paper and contains a critical evaluation of the overall system.

II. SYSTEM FEATURES

Generally, cloud storage service has different advantages and features due to the service that it provides. It's always paid when needed and sometimes is free according to the service that it provides; simply file hosting services such as Dropbox have no cost at the entry-level. In fact, Dropbox is free up to 2 GB of storage and maybe more due to some operations that the user can do such as inviting other users [2]. Most of the featured will be discussed in this section.

A. Dropbox Scalability

Cloud storage services are scalable and any device with a connection to the internet can use these services [2]. The number of Dropbox users is increasing daily, it reaches 275 million of users by the end of 2013 [11]. Dropbox achieves geographic scalability; any user can make his own account easily on his computer or smartphone. The user just needs a net connection on his device, and we know that the internet is widely used these days. Like any file hosting services, Dropbox has a central server that manages all uploading and downloading operations which support the scalability of this system.

B. Heterogeneity of Dropbox

Modern cloud-based applications including cloud storage services such as Dropbox are heterogeneous applications. They serve many edge clients such as laptops and smartphones.

The client's properties are different from one client to another; they may vary in hardware, software versions, operating system, network connection, and many other variations. This heterogeneity may degrade the performance of cloud-based applications [8].

Millions of users are served by modern data centers daily. Edge clients may use different hardware like high-end desktop computers and limited resources for smart phones. The operating system of the client's computers may also differ in the user type such as Linux, Mac OS, Android, and Windows. The network connection can be a wireless or wired network, and it also can be 3G or 2G networks. The software versions vary from one old version to the updated one (i.e. Dropbox 1.5.31 and Dropbox 2.6.31). All these differences in the client's platform characteristics cause the Dropbox to be a heterogeneous distributed system [8].

C. Dropbox Performance

Dropbox design is hybrid because it uses two types of servers; this allows effective use of cloud resources. EC2 servers are used for computation such as computing the hash values for the file chunks and content encryption. The Amazon S3 servers are used for storage and content delivery. The mix of the bandwidth of these services for both types of servers allow the operations of synchronization and collaboration of files to be easily done,

but the synchronization delay is increasing with expansion in Dropbox users and places.

Figure 1 shows that the synchronization delay in Dropbox cames from the large delay in the EC2 servers. The synchronization delay of the Amazon S3 servers is small compared with the EC2 servers. Some researchers did experiments to examine the Dropbox synchronization delay. They found that if they apply the content delivery of the Amazon S3 servers without any computation such as encryption and comparison that are done by the EC2 servers, the delay will be small compared with the delay of the real hybrid system [3].

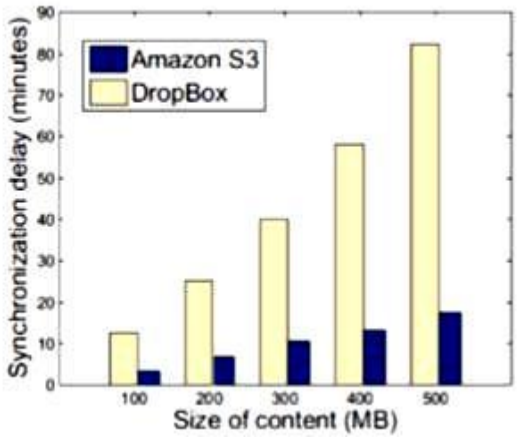

Fig. 1. Synchronization Dealy in Dropbox[3]

The Dropbox is heterogeneous and scalable distributed system and as we explained before, this heterogeneity may affect the performance and the quality of services from one client to another due to their platform characterization. Poor performance can be gained by poor characteristics of the client hardware, software versions, internet connection type and the used operating system. In addition, poor network connection of any type, including wireless and wired network results degradation in the system performance.

Performance of Dropbox and such cloud storage applications is affected by many factors that downgrade it on the edge client devices. The design of the software may be affected by certain assumptions that are taken by the developers, we can take the assumption of the maximum bandwidth of the network as an example and this may limit the size of the buffer that is allocated by the developers on the network stack, which means any upgrade to the bandwidth (from 2GB to 3GB) will make a big problem so many properties must be changed. In addition, the users always don't update their Dropbox software at new versions and this will cause inefficient implementation and bad performance. Finally, using the default configuration may also cause inefficient implementations [8].

D. The Openness of Dropbox

Dropbox can be described as an openness, distributed system. Any user can register in Dropbox and make his own account; it is not restricted to a group of users or special users. The basic Dropbox accounts, including the desktop and mobile applications are free, starting from 2GB of free space and this can be increased by different simple ways such as inviting friends to Dropbox or sometimes by giving extra information. As a result, any simple user can access the Dropbox application easily [5].

E. The Dropbox Security

Dropbox is an easy to use and it is user friendly, it is also secured with 256 bits AES and two verification steps and login authentication. Many attackers can retrieve the user files. The Dropbox uses the Amazon Web Services (AWS) as a data storage and it is able to encrypt files that the user uploaded by using encryption keys [10].

a) Stolen Host ID Attack

The host ID is a unique ID that is created when configure the Dropbox client application initially on the users' computer or smart phone, this ID binds the user device with his own Dropbox account. The host ID is also used for client and user authentication, since the Dropbox client software does not store user name and password. The Dropbox server randomly calculates the host ID which consists of 128 bits with some values that the client supplies such as a username or exact date.

There is no further authentication is required if the client is linked to the host that have the Dropbox software, thus linking need the user account username and password while the software is not removed from the host. If an attacker steals the host ID by using a malware or social engineering, he can retrieve every file in the local Dropbox of the originating user by resynchronization the folder.

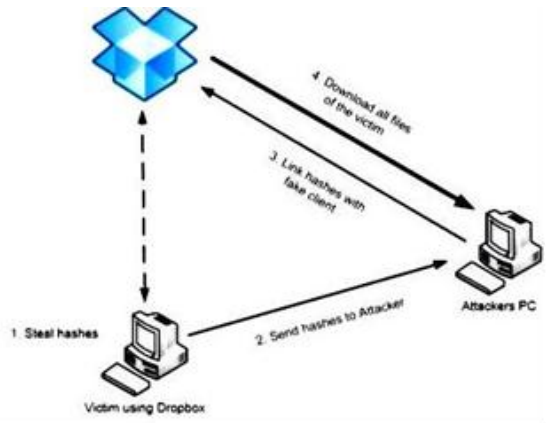

Fig. 2. Hash Value Manipulation attack [7].

b) Manipulation of the Hash Value Attack

The hash value attack is undetectable to the user; if the attacker has the hash value he can download files easily from the Dropbox server without any interaction with the client since no access to his computer is required to see Figure 2. The Dropbox server believes that the attacker has the files already and he wants to add them to his Dropbox local file on his device.

The Dropbox client is coded using Python language which has the hashlib library, but the SHA-256 hash value is calculated with open SSl using the NCrypto wrapper library and didn't use the Python hashlib library [7]. The library of the hash values on the Dropbox can replace and the Dropbox client cannot detect this replacement as Figure 3.

The Dropbox client for operating systems such as Linux and Mac OS X links to NCrypto libraries dynamically without any verification. If a modification is being done on NCrypto source code the attacker can replace his own hash values [7]. Here we can refer to the deduplication algorithm, To prevent the duplication when many users

send the same file; the hash values are compared to the stored hash values when the value already exists, then the related chunk also exists so the chunk will not be sent to the server [10]. If the hash value does not exist in the server database the server requests the client to send files/chunk and edits the hash value after transmission [7].

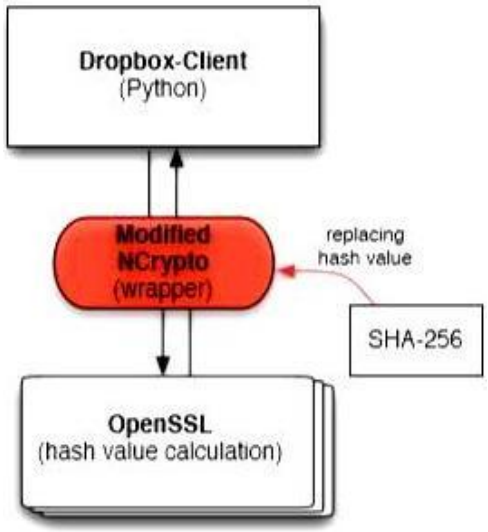

Fig. 3. Hash Value Replacement through the Modification [7].

TABLE I. Domain Name Used by Different Dropbox Services. Numeric Suffixes Are Replaced by X Letter [6].

sub-domain	Data-center	Description
client-lb/clientX	Dropbox	Meta-data
notifyX	Dropbox	Notifications
api	Dropbox	API control
www	Dropbox	Web servers
d	Dropbox	Event logs
dl	Amazon	Direct links
dl-clientX	Amazon	Client storage
dl-debugX	Amazon	Back-traces
dl-web	Amazon	Web storage
api-content	Amazon	API Storage

c) Direct Download Attack

The client software request chunks from server from clientX.Dropbox.com/retrieve as mentioned in Table1.The transmission protocols between the Dropbox client and server is built on HTTPS. This operation needs the SHA-256 hash value file chunks and the host Id as HTPPS POST to be submitted, any valid host ID can be used with the known hash value to retrieve files. The deletion of the files in Dropbox is a hard operation, so the attacker can easily retrieve the files with a valid host ID and a valid hash value. This attack can be detected by Dropbox since the host ID wasn't used to upload files before and just want to download files.

d) Developed Algorithms

Many developers proposed different algorithms to limit the unauthorized access of the user data. These algorithms are implemented in Android and web application such as serpent cryptographic, One-Time Password (OTP) and building a web application by using the Dropbox application programming interface (API) and bouncy castle library. Another new algorithm is named BoxLock which gets its name from Dropbox and the key lock, this method is used for file encryption as shown in Figure.

One-Time Password (OTP) indicates that every user has more than one password, and in each transaction operation the user can use a different password. In the OTP the password is different in each interval of time. The password can be generated by the user using a button in the OTP device each time. This algorithm provides event-based OTP codes. The serpent is an encryption Algorithm that uses symmetric encryptions [10].

There is a middleware layer that handles the authentication processes of the Dropbox application on a device such as mobiles, this middleware works in the real-time as traffic avoidance in the HTTP. Infrastructure-as-a-service (IaaS) cloud uses their services APIs to facilitate applications on devices such as mobiles. The middleware uses the OAuth 2.0 techniques to identify the security in order to support authentication with the IaaS in addition to data protection to the end-users [9].

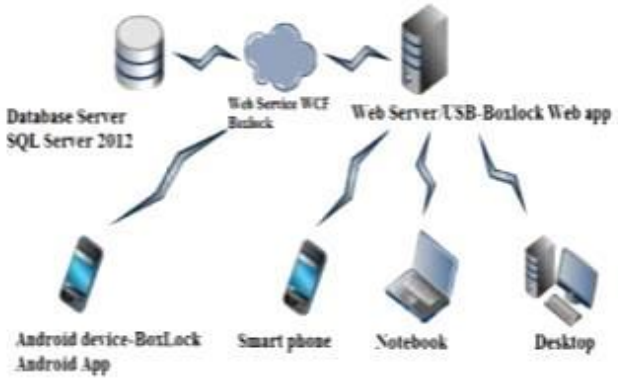

Fig. 4. BoxLock system Architecture

D. Transparency of Dropbox

The Dropbox client protocols information is mostly hidden due to hidden communications and the encryption which is done on the transport layer security, these steps are done to ensure the transparency and the security of the Dropbox. The general operations that cause the communications are summarized by adding or removing files on the local Dropbox folder, downloading new files and creating new folders [6]. The communication of the Dropbox system is done among the TCP socket [8].

E. Reliability and Fault Tolerance of Dropbox

Dropbox is a popular file hosting service nowadays; it is used widely all over the world. Dropbox is known as reliable file storage and is also known as an effective application used for file synchronization and collaboration among multiple users [3]. All the client/ server communications are done via TCP sockets to ensure reliability [8].

Files in cloud storage systems such as Dropbox and ICloud are available and accessible in contrast to local file systems. The reliability of such systems is achieved through data redundancy; this redundancy is satisfied by file replication on multiple storage devices or nodes. Many mechanisms are used to manage and distribute file replicas among storage nodes such as RAID mechanism, network coding and erasure code. Each of the previous mechanisms supports redundancy and fault tolerance [13].

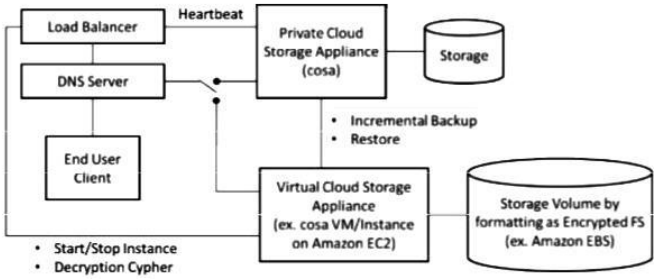

Fig. 5. The Hybrid Storage Service Architecture [14].

III. SYSTEM DESIGN

Dropbox is one of the most popular cloud storage services. It monitors a particular local folders, which are located on the client computers or other devices, replicates the content of these local folders to all folders that the user shares the content with them, maybe all the devices, including computers having the same local Dropbox folder owned by the same user who running the desktop client [2].

Dropbox can be also seen as a synchronization service for files/folders, when a user shares a file/folder in the local Dropbox folder you may wait some time, which depends on the size and the bandwidth of the file/folder then you can see the shared file/folder from all clients and this is what we meant by the file/folder synchronization. Some desktop clients have an icon on the lower right corner indicates that there is a folder being synchronized now if the icon shows a blue rotating arrow if the icon shows a green tick which indicates that the file/folder is now ready and completes synchronization operations [2].

In order to achieve high availability operations for Dropbox system, a hybrid storage service is designed. Figure 5 shows the architecture of this hybrid system [14]. Like any distributed system Dropbox consists of many parts like clients, servers, and database, in this research I will describe each component with detailed information and how they interact with each other [6].

a) The Dropbox Service Framework

Dropbox is a distrusted system that uses as a file hosting services which is used for collaboration and synchronization files among multiple users in different places and different devices. As any distributed system Dropbox consists of components such as clients, servers and databases. Figure 6 shows the main components of the Dropbox service framework. The first component is the load balancer which includes six IP addresses 199.47.216.172-174 and 199.47.217.172-174, these six load balancers are managed by the Dropbox.

Domain v-client.sjc.Dropbox.com. Other components are EC2 servers which are used for computation operations such as downloading, uploading and file processing like comparison and encryption. 360 EC2 servers are used in the Dropbox service from dl-client1.Dropbox.com to dlclient360.Dropbox.com which you can see in Table 1, the number of the EC2 server is denoted by X letter. 260 of the EC2 servers are active and do the computation while the remaining 100 are used for backup operations. The S3 components are corresponding to the Amazon servers which are storage servers used as database storage for the Dropbox service [3].

The communication between the users and the S3 servers is done among the EC2 servers. When a source client wants to upload a file on his own Dropbox folder, the user will send a DNS request to ask about the IP address of the domain v-client.sjc.Dropbox.com which is the load balancer of Dropbox. The DNS replies with the six load balancers of this domain name. The source client will choose one of the load balancers randomly and sends it the file information such as file size, type and etc. The load balancer will assign an EC2 server to the client to allow the client to upload the file to this assigned EC2 server. Finally, the EC2 server will forward the uploaded file to the S3 server especially to the client's folder and then to the destinations that need to be synchronized [3].

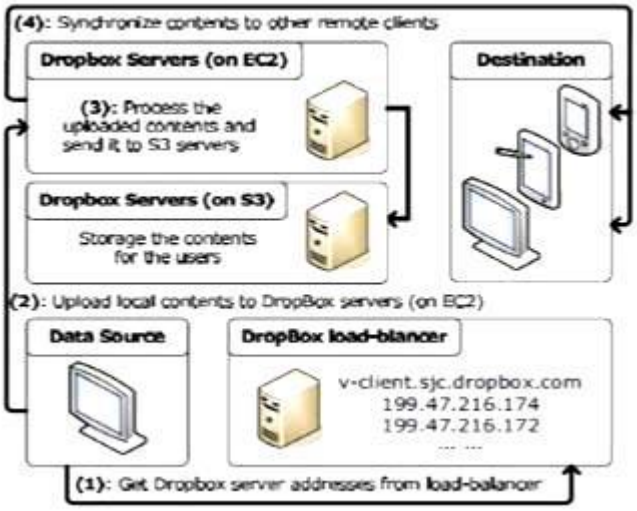

Fig. 6. The Dropbox Framework [3]

B. The Dropbox Client

Large parts of the Dropbox client are implemented in Python, which is a high-level programming language used for general purpose applications with fewer lines of code that could be written in other languages [12], it also uses the third-party libraries like librsync which is a software library that is presented for free and used to implement sync remote_dat algorithms that permits remote updates of files.

The Dropbox application software is available and compatible with many operating systems such as Microsoft Windows, Apple OS X, and Linux. All data is synchronized with servers, and all changes of the client data are also synchronized automatically to all other clients. Each client has an account which can be accessed from any linked client device among the internet, and this account is used to share folders [6, 7].

In the Dropbox distributed system the file is not the main used concept, while chunk is the basic object in this system. Each chunk has a size of 4 MB or less, according to the shared file sizes if the file is larger than 4 MB it is split into more than one chunk. Adding a file to the local Dropbox folder prompts the Dropbox client to identify each chunk by using a hash value of SHA-256 algorithm; this hash value is part of the metadata that describes the file [6, 7].

To prevent the duplication when many users send the same file; the hash values are compared to the stored hash values when the value already exists, then the related chunk also exists so the chunk will not be sent to the server. And this operation is named deduplication algorithm [10]. The amount of exchanged data is reduced by using delta encoding while transmitting chunks. Each device that has

the same Dropbox account keeps the meta-data information that describes the sharing files and it is updated via incremental updates. The chunks are compressed usually before submitting them to be transmitted as easy as possible [6].

C. The Dropbox Server

Besides the local file of the Dropbox there is a daemon that checks if a file/folder created or updated and uploads it to the server, this daemon also replays on the Dropbox server requests by uploading file/folder from the central server to the local Dropbox server. Like any file hosting services, Dropbox has a central server that manages all uploading and downloading operations. The synchronization operation takes some time according to the file size and bandwidth, the client may see that files are synchronized from one node to another under the user control. File replication or updating is seamless for the client but in fact, it is slow, and to make it fast enough they have coded all the file names information so the information is to be transferred downstream to the nodes and upstream to the server [2].

In fact, many servers are responsible for Dropbox client's protocols to perform typical tasks such as file synchronization.

These tasks are distributed among the Dropbox servers, this operation of load distribution among servers is done by supporting different list of the DNS to each client and a rotating IP addresses among the responses DNS as we mentioned before [6].

D. Dropbox Communication

In this system, the transactions are done between the client and the server such as file downloading from the server and uploading from the client. Figure 7 shows the client/ server communication architecture. The server can log some information such as the used operating system, the program that used to download the files and the total time needed to download the data. The server needs this information to compute the time needed by the clients and to compare each client time with others. The previous comparisons are used to cluster nodes, this is done dynamically.

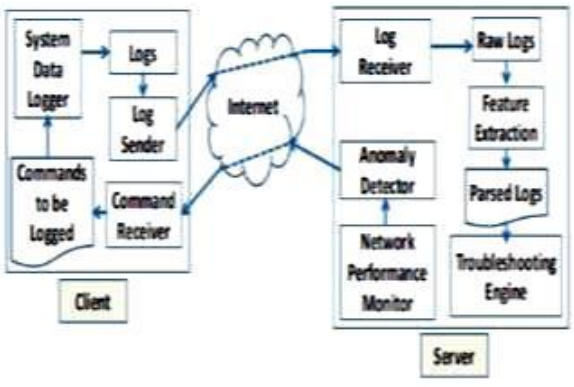

Fig. 7. The Client/Server Communication Architecture [8].

The client must know the IP address or the URL of the server, it is told which command log for reference to the server by Linux commands and this may be done manually. The log is sent by the client to the server after the completion of the execution. All client/server communications are done via TCP sockets to ensure the reliability of the logs transactions. The server listens to many logs came from different clients, while the client listens to the commands came from the server [8].

The Dropbox client protocols information is mostly hidden due to hidden communications and the encryption which is done on the transport layer security, these steps are done to ensure the security of the Dropbox. The general operations that cause the communications are summarized by adding or removing files on the local Dropbox folder, downloading new files and creating new folders [6]. Table 1 shows the sub-domains of Dropbox.com that used for the communications when executing the previous Dropbox operations. An example of the Dropbox protocol communication is shown in the figure bellow.

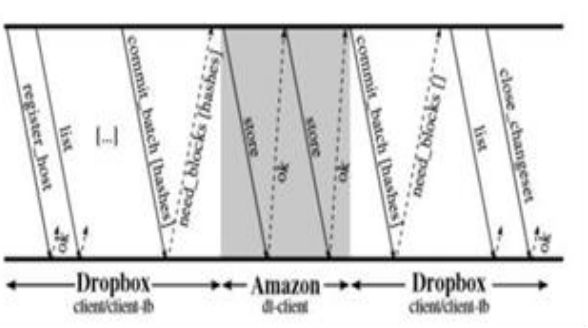

Fig. 8. An Example of a Dropbox Protocol [6].

First of all the user must register with the Dropbox control center at the Dropbox server (client.Dropbox.com) and then retrieve the meta-data which include all information about the chunks and the file, this operation is done by the list command. When a new file is added to the local Dropbox folder, the metadata information is instantaneously submitted by commit-batch command via the meta-data sub-domain for Dropbox (clientlb.Dropbox.com).

The store command then stores on the Amazon servers on (dlclientX.Dropbox.com). An ok acknowledgment is received after each chunk store operation. Finally, after a successful submission, the client sends messages to the central Dropbox server (clientlb.Dropbox.com) to indicate that a transaction is completed and committed; this step can be done at the time of the store operation [6]. Figure 9 shows the system flow including uploading/downloading files in Dropbox starting with user registration, and also including the security insurance [10].

IV. SECURITY RELATED WORKS

Several solutions were proposed during the last decade to address the challenges and problems to secure the cloud storage; this section focuses on the most important research in this field:

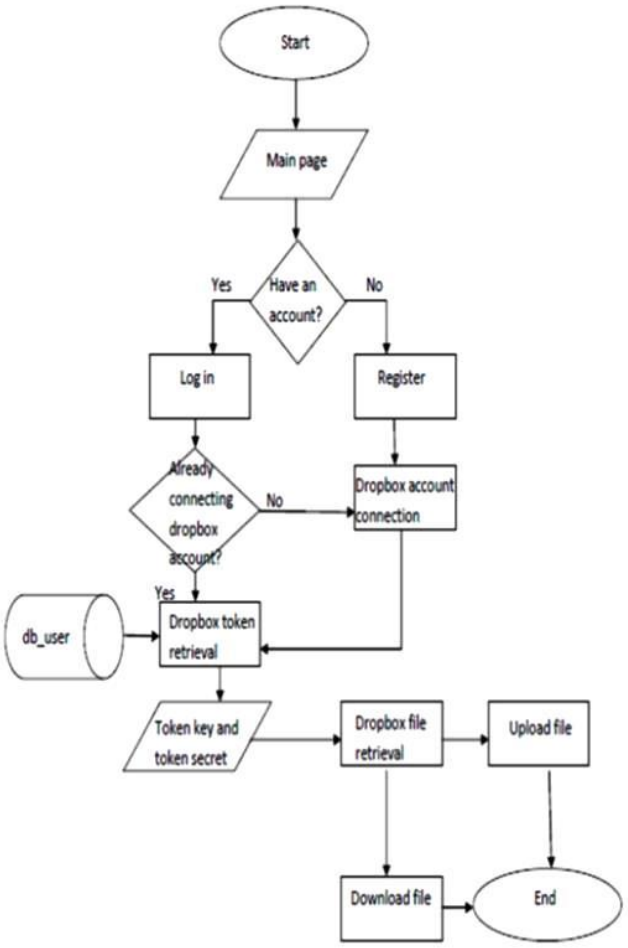

Fig. 9. Dropbox General System Flow [10].

Burihabwa et.al in [15] designs a practical experience report to study the wide range of security mechanisms that can be used to protect data in cloud-based storage services. And They also evaluate and discuss several security techniques' that can be used in the implementation and design the safe store system to evaluate the performance trade-offs of the security and deployed across several standard cloud-based storage services. and study the relationship between the performance and memory overhead, and prove that the CPU overhead increase with the increase of security levels.

Sandeep and Vaidya in [16], design a system that authenticates users, and use storage cloud systems like Dropbox as backend storage. By Providing a security layer over the storage system and applying slicing algorithm on the file to split it into three segments then encrypt those segments by encryption algorithm, then upload them to the cloud storage, and` when needed the segments decrypted and then merged by the merging algorithm to reconstruct the original file and return it to the user. Bruce Wu in [17], present a RAM analysis based method to extract the key security token for account access. Also, they discuss a new approach by using tray_login feature to bypass authentication access to Dropbox accounts, and finally they describe potential resolutions that can improve Drop box's security.There are two popular ways to protect data, the way that is used in Dropbox is to upload the cloud data then encrypt it using encryption algorithm. But in [18] the author describes a second way to protect data, by designing an implementation of HCPOD (Hierarchical) client on top of a cloud CRM which is encrypts then upload.

Because there is a lot of transfer data between applications and database in thecloud, so it needs to be faster, they proposed a method that add algorithms and logics to the existing. This work concentrates more on the performance of Encryption and decryption as enterprise application involves Lot of transactional data.

Shin *et.al* in [19] think that the cloud service such as Dropbox that offers server-side data encryption for security is not secure enough because all the encryption keys are managed by software, so they implement a framework to fix this problem named DFCloud, that secure the data access in cloud storage service in mobile devices, they study the data leakage problem and exploits Client-side encryption technique to mitigate server-side data leakages, build a secure access environment and support secure key sharing protocol across the devices or clients', the result show that the performance has a quit overhead.

To ensure the security of a cloud storage service, all communications between users and the cloud storage service are encrypted, so nobody can get the data during uploading or downloading. In [20] Chu et.al, compare three popular cloud storages. Dropbox, Google Drive, and Microsoft SkyDrive and discuss some of the weakness for each one of them while data sharing. They discuss some of the weakness points in Dropbox such that Non-dead URL for the shared data, another one is Non-HTTPS shortened URL means that if the user asked for a URL using Smartphone the Dropbox application may generate a shorted URL in an HTTP form to make it easy for the user to send the URL using messages or Bluetooth. also the Unauthorized re-sharing means when the user shares a file with another user, the second one may share the folder with people by using a secrete URL or by downloading the folder. Also, no privacy on sharing means that anyone access the shared folder can see the identities of the other people. And the final one is uncertain identities that mean that for private sharing, if the user sends the invitation to an email address hasn't been registered on Dropbox, he can follow the invitation link to register a new account with any email address to access the sharing folder.

There are two important things have to be studied in cloud storage the first is the cloud security and the second is the Forensics investigation in the cloud, in [21] the authors study the forensics investigation and try to get more information about the criminals that use the cloud service for illegal purposes. They use Wireshark to analyze network traffic log files after working with cloud software to determine the details of activities in the cloud. They also used the existing forensics tools such as Pro-Discover Basic and methodologies to retrieve the artifacts of cloud activities such as edit, delete, and upload of files to the cloud storage services such as Dropbox. They also used Pro-Discover Basic computer forensics tool to make an image of the Dropbox Folder. And then used the same tool to acquire, and analyze forensics artifacts of the Dropbox cloud service. The results show that the use for forensics techniques and tools reveal much More information about a suspect's use of cloud storage services, such as file access history, user Id of the person who accessed the file, actions that were performed on the file, etc.

In another point of view, Kholia and W˛egrzyn in [22] implemented an open source Dropbox to make the Dropbox available for all researchers and security analysis, also they implement a method to bypass

Dropbox's two factor authentication and hijack Dropbox accounts.

Sari.A in [23] describes the importance of anomaly detection system in the cloud environment, he surveys its types, methods, and the limitations. These limitations can create inaccuracy in anomaly detection. He compared between the different security measurements of cloud storage services such as Dropbox, Google Drive, and iCloud; he shows that the Dropbox is the most secure cloud storage, but for storage the Google-Drive is the best.

Ko.A and Zaw.W in [24] proposed a cloud storage forensic and use Dropbox as a case study and describe a lot of information that can be found by analyzing artificial left by cloud storage client ,they also documented a series of digital forensic that they created experiments with the aim of providing forensic practitioners to undertake the cloud storage forensics.

V. CONCLUSIONS

Recently, Dropbox became a popular cloud storage application with a high number of users that reach 275 millions of users by this year and this number is increasing yearly. The Dropbox traffic on the network is equivalent to one-third of the YouTube traffic. Dropbox is a file-sharing program, it is like a pool that you can drop your files, images, videos on it and you can access them from anywhere using the internet. There is a local folder on the client computer or smartphone that he can access his files/folders through it, but in fact there are huge data centers that contain all the client information. The client must connect with the central server to retrieve or upload his staff. The communication among the clients and servers is done by using special primitives and special communication protocols.

Dropbox uses the Amazon storage data centers; it stores the data on Amazon S3 storage service that is part of the Amazon Web Services (AWS). The file is split into chunks and each chunk is uploaded/ downloaded alone, each chunk has meta-data information to bind each chunk with others on the same file and it also contains information about the synchronization process. The servers are distributed among the regions and each client connects to maybe the nearest server, and the server can be selected due to the uploaded/downloaded files information such as file size and type.

In this paper, we presented the Dropbox features as a distributed system and we find that the Dropbox is openness system and anyone can create an account on the Dropbox system and enter his own registration information any time, since that the Dropbox is free starting from 2GB free space and maybe more. The overall system performance of the Dropbox is high due to some improvement in the system and due to good communication and ease of use, but there are some defects occurred in the performance because of the fault developers assumptions that must be changed with the improvements of the system and also because of the edge client users incorrect using of the application.

The Dropbox is a scalable system which is widely distributed among the world; it is also a heterogeneous system because of many differences on each edge client platform characteristics. The Dropbox is a transparent system, all the communication within it is hidden and the transmitted data are encrypted via the transport layer. Many algorithms are improved to ensure the security of the Dropbox system. Serpent decryption OTP and BoxLock are all developed to increase system security and to avoid file attacks.

The main problem in the Dropbox system is the long synchronization delay. This delay is come from using multiple servers in different places. In my opinion, I see if the Dropbox can do the computation and storage services in the same servers the delay can be controlled. This adds a load on the storage servers, it may be not applicable.

Another idea is to synchronize the files directly to the Amazon S3 servers without using the EC2 servers, the computation may be done on the same client by additional operations.

REFERENCES

[1] Zurita, Gustavo, Nelson Baloian, and Jonathan Frez. "Using the cloud to develop applications supporting geocollaborative Situated Learning." Future Generation Computer Systems 2013.

[2] Garcia-Arenas, M., J-J. Merelo, Antonio Miguel Mora, Pedro Castillo, Gustavo Romero, and Juan Luís Jiménez Laredo. "Assessing speed-ups in commodity cloud storage services for distributed evolutionary algorithms." In Evolutionary Computation (CEC), 2011 IEEE Congress on, pp. 304-311. IEEE, 2011.

[3] Wang, Haiyang, Ryan Shea, Feng Wang, and Jiangchuan Liu. "On the impact of virtualization on Dropboxlike cloud file storage/synchronization services." In Proceedings of the 2012 IEEE 20th International Workshop on Quality of Service, p. 11. IEEE Press, 2012.

[4] Wikipedia, Cloud storage, "en.wikipedia.org/wiki/cloud_storage." , 5 April 2014.

[5] Dropbox, Tour, " https://www.Dropbox.com/tour. ", 201.

[6] Drago, Idilio, Marco Mellia, Maurizio M Munafo, Anna Sperotto, Ramin Sadre, and Aiko Pras. "Inside Dropbox: understanding personal cloud storage services." In Proceedings of the 2012 ACM conference on Internet measurement conference, pp. 481-494. ACM, 2012.

[7] Mulazzani, Martin, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar Weippl. "Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space." In USENIX Security Symposium. 2011.

[8] Fagan, Michael, Mohammad Mai Khan, and Bing Wang. "Leveraging Cloud Infrastructure for Troubleshooting Edge Computing Systems." In Proceedings of the 2012 IEEE 18th International Conference on Parallel and Distributed Systems, pp. 440-447. IEEE Computer Society, 2012.

[9] LOMOTEY, Richard K.; DETERS, Ralph. SaaS Authentication Middleware for Mobile Consumers of IaaS Cloud. In: Services (SERVICES), 203 IEEE Ninth World Congress on. p. 448-455. IEEE, 2013.

[10] Yulianto, Aditya, S. Kom, and Maria Irmina Prasetiyowati. "BoxLock: Mobile-based Serpent cryptographic algorithm and One-Time Password mechanism implementation for Dropbox files security." In Information Science and Technology

(ICIST), 2013 International Conference on, pp. 357362. IEEE, 2013.

[11] Dropbox, Highlights, "www.Dropbox.com/news." 22 Jan 2014.

[12] Wikipedia,Python(programminglangwage,"http://en.wikipedia.org/wi ki/ python-(programming-langwage)." 14 May 2014.

[13] Mohammad Reza Zakerinasab, Mae Wang. "An Apdate Model for Network Coding in Cloud Storage System." In Allerton Conference, 2013 LLLinois 15th Annual, 1-5, 2012.

[14] Kuo, Yen-Hung, Yu-Lin Jeng, and Juei-Nan Chen. "A Hybrid Cloud Storage Architecture for Service Operational High Availability." In Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual, pp. 487-492. IEEE, 2013.

[15] Burihabwa, D., Pontes, R., Felber, P., Maia, F., Mercier, H., Oliveira, R., ... & Schiavoni, V. (2016, September). On the Cost of Safe Storage for Public Clouds: an Experimental Evaluation. In Reliable Distributed Systems (SRDS), 2016 IEEE 35th Symposium on (pp. 157-166). IEEE.

[16] Vaidya, M. B., & Nehe, S. (2015, December). Data security using data slicing over storage clouds. In Information Processing (ICIP), 2015 International Conference on (pp. 322-325). IEEE.

[17] Wu, B., Nguyen, T., & Husain, M. (2015, April). Implementation vulnerability associated with OAuth 2.0--A case study on Dropbox. In Information Technology-New Generations (ITNG), 2015 12th International Conference on (pp. 135-138). IEEE.

[18] Vanitha, M., & Kavitha, C. (2016, January). Performance enhanced security for enterprise cloud application. In Computer Communication and Informatics (ICCCI), 2016 International Conference on (pp. 1-5). IEEE.

[19] Shin, J., Kim, Y., Park, W., & Park, C. (2012, December). DFCloud: A TPM-based secure data access control method of cloud storage in mobile devices. In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on (pp. 551-556). IEEE.

[20] Chu, C. K., Zhu, W. T., Han, J., Liu, J. K., Xu, J., & Zhou, J. (2018). Security concerns in popular cloud storage services. IEEE Pervasive Computing, 12(4), 50-57.

[21] Ghafarian, A. (2015, July). Foreniscs analysis of cloud computing services. In Science and Information Conference (SAI), 2015 (pp. 1335-1339). IEEE.

[22] Kholia, D., & Węgrzyn, P. (2017). Looking inside the (Drop) box. In Presented as part of the 7th USENIX Workshop on Offensive Technologies.

[23] Sari, A. (2015). A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security, 6(02), 142.

[24] Ko, A. C., & Zaw, W. T. (2018). Digital Forensic Investigation of Dropbox Cloud Storage Service. Network Security and Communication Engineering (Ed: Kennis Chan), CRC Press: İngiltere, 147-150.