The Study of the Application of Data Encryption Techniques in Cloud Storage to Ensure Stored Data Integrity and Availability

Okeke Stephen

Department of Computer Science, College of Physical and Applied Sciences, Michael Okpara University of Agriculture, Nigeria.

Abstract- Nowadays, the rates of malicious data theft and data destruction are alarming. Governments, companies and other organizations have lost a lot of money and many others have closed down due to the activities of dubious hackers and attackers. As data is the life wire of every organization, there is the need to remotely and securely store the data generated daily by these organizations in order to enable them recover quickly in the event of attach and hack. Cloud storage is needed here for the remote data storage. For many establishments, data security is one of their major concern when sending their files into the cloud. They worry about their files being seen or even compromised by malicious and dubious people because that's what happened in the past. User accounts have been hacked, cloud storage systems failed, files and personal data were exposed. So how can you effectively prevent that from happening even if your account gets hacked or something happens to your cloud storage provider. Data encryption techniques are required to protect the integrity of the stored data. In the past, many businesses felt comfortable allowing the cloud providers to manage all their data, believing that security risks could be managed through contracts, controls and audits. Over time it has become apparent, however, that cloud providers cannot honor such commitments when responding to government requests for information. In this paper, I will focus on cloud storage providers, cloud security challenges, encryption methodologies.

Index Terms- Cloud Storage, Encryption, Cipher text, Symmetric and Asymmetric encryptions.

I. Introduction

Cloud Storage is a system whereby data is remotely stored, maintained, managed, and backed up. The service is available to users over a network, which is usually the internet. It allows the user to store files online so that the user can access them from any location through the internet. The service providing company makes them available to the user online by keeping the uploaded files on an external server. This gives companies using cloud storage services ease and convenience, but can potentially be costly. Storing data safely offsite is one of the cloud's key features. Studies have found that fully 80% of businesses that suffer major data loss go out of business within two years. This is where cloud storage has generated the most interest because it allows you to safely store critical data on a public or private cloud.

These off-site, proven production systems are managed by trained and experienced admins that few businesses could otherwise afford themselves. Cloud Storage has also been increasing in popularity recently due to many of the same reasons as Cloud Computing. Cloud Storage delivers virtualized storage on demand, over a network based on a request for a given quality of service (QoS). There is no need to purchase storage or in some cases even provision it before storing data. You only pay for the amount of storage your data is actually consuming. Cloud storage is used in many different ways. For example: local data (such as on a laptop) can be backed up to cloud storage; a virtual disk can be "synched" to the cloud and distributed to other computers; and the cloud can be used as an archive to retain (under policy) data for regulatory or other purposes.

For applications that provide data directly to their clients via the network, cloud storage can be used to store that data and the client can be redirected to a location at the cloud storage provider for the data. Media such as audio and video files are an example of this, and the network requirements for streaming data files can be made to scale in order to meet the demand without affecting the application. The type of interface used for this is just HTTP. Fetching the file can be done from a browser without having to do any special coding, and the correct application is invoked automatically. But how do you get the file there in the first place and how do you make sure the storage you use is of the right type and QoS? Again many offerings expose an interface for these operations, and it's not surprising that many of these interfaces use REST principals as well. This is typically a data object interface with operations for creating, reading, updating and deleting the individual data objects via HTTP operations.

II. THE BRIEF EVOLUTION OF CLOUD STORAGE

Over the last few years, the capabilities and reach of cloud storage services have evolved rapidly, with many organizations expressing interest in storage-as-a-service. Cloud storage is a subcategory of the very complex cloud computing idea. It is a service model in which data is: maintained, managed and backed up remotely and made available to users over a network (typically the Internet). FilesAnywhere.com was one of the first companies to offer the cloud storage service. Their cloud storage service enabled users to store data on their servers from anywhere at any time, while also being able to retrieve the data from anywhere at any time. FilesAnywhere.com would be a pioneer in the cloud storage business and many companies would follow suit.

Figure1 Evolution of Cloude Storage

III. CLOUD STORAGE ARCHITECTURES

Cloud storage architectures are primarily about delivery of storage on demand in a highly scalable and multi-tenant way. Generically, cloud storage architectures consist of a front end that exports an API to access the storage. In traditional storage systems, this API is the SCSI protocol; but in the cloud, these protocols are evolving. There, you can find Web service front ends, file-based front ends, and even more traditional front ends (such as Internet SCSI, or iSCSI). Behind the front end is a layer of middleware that I call the storage logic. This layer implements a variety of features, such as replication and data reduction, over the traditional data-placement algorithms (with consideration for geographic placement). Finally, the back end implements the physical storage for data. This may be an internal protocol that implements specific features or a traditional back end to the physical disks.

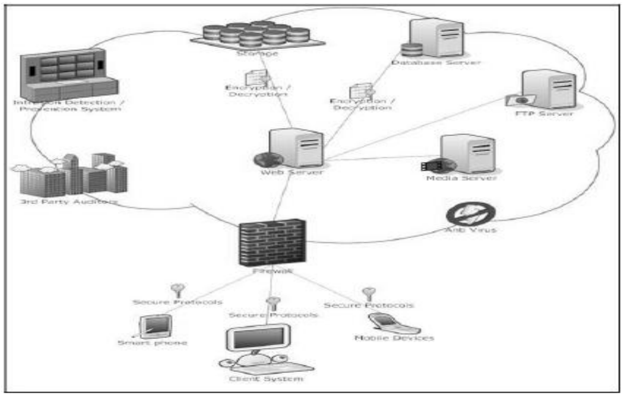


Figure2 Cloud Storage Achitecture

IV. CLOUD STORAGE PROVIDERS AND THEIR FEATURES

They are many cloud service providers. Generally, these service providers normally give out free storage space to a certain number of gigabytes, after which monthly fee subscription commence. The cloud storage service providers provide drag-and-drop accessing option and syncing of folders and files between a desktop and mobile devices, and the cloud drive. They also allow all account users to collaborate with each other on documents. The major providers are:

Figure3 Cloud Storage Providers

Box

Collaboration: You can share content with both colleagues that do have Box accounts, and those who don't. Like Dropbox, you can create a shared folder and invite Box account colleagues for ongoing sharing. You can receive email notifications when files are uploaded, downloaded, or added. You can also set passwords for important files and set time limits for user access to certain files. You have more control over user access to files and documents because security levels can be defined. Box is geared more towards businesses and enterprises, but it is also available for personal use.

Mobile App Support: Users can view, edit, create and share content on-the-go. You can find files fast with built-in search. It allows you to save files you create or edit in other apps to your Box account. You can also upload files from your phone or tablet to Box as well as save files from Box onto your mobile device for offline access.

Storage: Box offers 5 GB of free storage.

Strengths: You can store larger file sizes. Box is organized and user friendly, you can create and organize several layers of folders for all of your documents and data. You can use tagging as a way to keep track of your folders and files. Tags allow you to mark and sort related files that may not be located in the same section of your Box. Box offers the highest security options. Content management tools.

Weaknesses: Box doesn't do file-syncing from the computer to box.com as simply as other services do. There is a desktop component called Box Sync, but it's available only to Business and Enterprise account holders for a fee.

Google Drive

Collaboration: Users of Google Drive documents must have a Google Drive account. All updates and editing by collaborators will be synced to Google Drive. For documents that you have permission to access, you can receive notifications when changes are made. You can share files with people by sending them a link to your file.

Mobile App Support: Google Drive has an Android app which gives you the ability to share the files on your Android device using your Drive account. You can also share any file from Drive with your phone contacts.

Storage: Google Drive offers 5GB of free storage.

Strengths: Has built-in document editor so that programs such as Microsoft Word are not required to be installed on computer in order to edit document. Allows comments to be left on any files stored.

Weaknesses: Sharing not as easy and intuitive as Dropbox—must use the Google Drive web application to set it up. Also no ability to set preferences on syncing speed.

Microsoft SkyDrive

Collaboration: Colleagues can access SkyDrive files without having to sign up for a SkyDrive account. You can also update documents simultaneously online with colleagues.

Mobile App Support: SkyDrive offers both a Window's phone app and an iOS (iPhone/iPad) app. This allows users to view and share as well as edit and update files via phone or tablet. SkyDrive files can also be opened using third party iOS apps, such as Pages and Keynote.

Storage: SkyDrive offers 7GB of free space.

Strengths: Offers the most storage for free of the options reviewed in this document. Like Google Drive, you can edit documents within the browser, without having to open up a client application like Microsoft Word.

Weaknesses: – Skydrive is somewhat less user friendly than Dropbox and Google Drive.

Dropbox

Collaboration: Dropbox gives users the capability of sharing entire folders with other Dropbox account users, which allows updates to be viewable by all collaborators. Users can download shared documents directly from Dropbox's web interface without having to install the Dropbox desktop client. Storing files in the Dropbox "Public" folder allows links to files to be sent to Dropbox and non-Dropbox users; however non-Dropbox link recipients must download the file to access/edit it, and any changes or revisions made to the file by the link-recipients will not be reflected in the Dropbox version of the file.

Mobile App Support: Documents are easily accessible through phone and tablets using the Dropbox mobile app.

Storage: Dropbox offers 2GB of free storage.

Strengths: Primarily in its ease of use. Very intuitive interface—for example, sharing folders is available by simply right-clicking the file or folder on the desktop, and choosing Sharing. You can also determine how fast files are synced in Preferences (right-clicking the Dropbox icon). You can also recover deleted files in Dropbox easier than some other options.

Weaknesses: Lowest amount of free storage of the offerings reviewed in this document. Also, when inviting users to share files/folders, the email invitation must be sent to the email address that is associated with the users' Dropbox account.

- **Pros of Cloud Storage**

Usability – All cloud storage services reviewed in this topic have desktop folders for Mac's and PC's. This allows users to drag and drop files between the cloud storage and their local storage.

Bandwidth – You can avoid emailing files to individuals and instead send a web link to recipients through your email.

Accessibility – Stored files can be accessed from anywhere via Internet connection.

Disaster Recovery – It is highly recommended that businesses have an emergency back-up plan ready in the case of an emergency. Cloud storage can be used as a back-up plan by businesses by providing a second copy of important files. These files are stored at a remote location and can be accessed through an internet connection.

Cost Savings – Businesses and organizations can often reduce annual operating costs by using cloud storage; cloud storage costs about 3 cents per gigabyte to store data internally. Users can see additional cost savings because it does not require internal power to store information remotely.

- **Cons of Cloud Storage**

Usability – Be careful when using drag/drop to move a document into the cloud storage folder. This will permanently move your document from its original folder to the cloud storage location. Do a copy and paste instead of drag/drop if you want to retain the document's original location in addition to moving a copy onto the cloud storage folder.

Bandwidth – Several cloud storage services have a specific bandwidth allowance. If an organization surpasses the given allowance, the additional charges could be significant. However, some providers allow unlimited bandwidth. This is a factor that companies should consider when looking at a cloud storage provider.

Accessibility – If you have no internet connection, you have no access to your data.

Data Security – There are concerns with the safety and privacy of important data stored remotely. The possibility of private data commingling with other organizations makes some businesses uneasy.

Software – If you want to be able to manipulate your files locally through multiple devices, you'll need to download the service on all devices.

V. CLOUD DATA ENCRYPTION

Encryption is the process of making files or data unreadable with an encryption key or pass phrase so that even if somebody gains access to the files – it doesn't matter because the only thing an intruder sees is gibberish. Only with the key you can properly see what's in a file. Cloud encryption is a service offered by cloud storage providers whereby data, or text, is transformed using encryption algorithms and is then placed on a storage cloud. It is the transformation of a cloud service customer's data into ciphertext. Cloud encryption is almost identical to in-house encryption with one important difference -- the cloud customer must take time to learn about the provider's policies and procedures for encryption and encryption key management. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted. Because encryption consumes more processor overhead, many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers. At this point in time, having the provider encrypt a customer's entire database can become so expensive that it may make more sense to store the data in-house or encrypt the data before sending it to the cloud. To keep costs low, some cloud providers have been offering alternatives to encryption that don't require as much processing power. These techniques include redacting or obfuscating data that needs to remain confidential or the use of proprietary encryption algorithms created by the vendor.

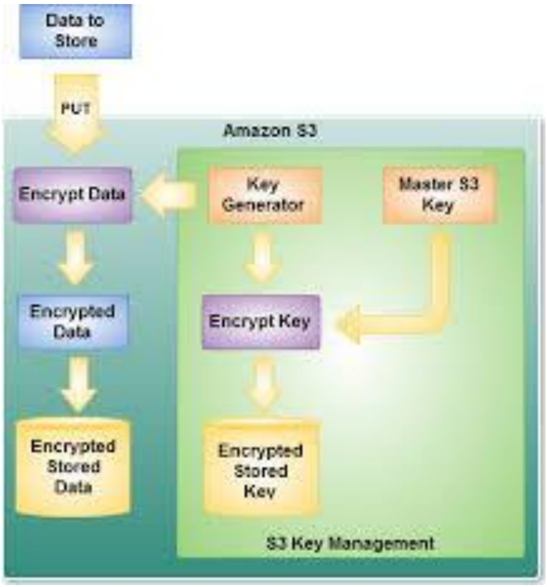


Figure4 Cloud Data Encryption

VI. CLOUD DATA ENCRYPTION METHODS

- **Cipher Text**

In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information from plain text into cipher or code. In non-technical usage, a 'cipher' is the same thing as a 'code'; however, the concepts are distinct in cryptography. In classical cryptography, ciphers were distinguished from codes. Codes generally substitute different length strings of characters in the output, while ciphers generally substitute the same number of characters as are input. There are exceptions and some cipher systems may use slightly more, or fewer, characters when output versus the number that were input.

Codes operated by substituting according to a large codebook which linked a random string of characters or numbers to a word or phrase. For example, "UQJHSE" could be the code for "Proceed to the following coordinates". When using a cipher the original information is known as plaintext, and the encrypted form as ciphertext. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it.

Block Ciphers and Stream Ciphers

One of the main categorization methods for encryption techniques commonly used is based on the form of the input data they operate on. The two types are Block Cipher and Stream Cipher. This section discusses the main features in the two types, operation mode, and compares between them in terms of security and performance.

Block Cipher

In this method ciphering, data is encrypted and decrypted if data is in from of blocks. In its simplest mode, you divide the plain text into blocks which are then fed into the cipher system to produce blocks of cipher text. ECB(Electronic Codebook Mode) is the basic form of block cipher where data blocks are encrypted directly to generate its correspondent ciphered blocks. More discussion about modes of operations will be discussed later.

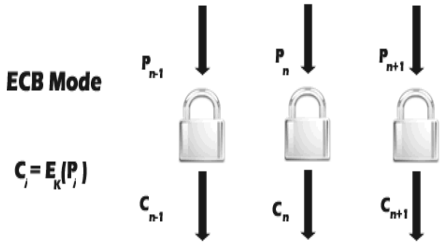


Figure5 Block Cipher ECB Mode

Stream Ciphers

Stream cipher functions on a stream of data by operating on it bit by bit. Stream cipher consists of two major components: a key stream generator, and a mixing function. Mixing function is usually just an XOR function, while key stream generator is the main unit in stream cipher encryption technique. For example, if the key stream generator produces a series of zeros, the outputted ciphered stream will be identical to the original plain text. Figure 3 shows the operation of the simple mode in stream cipher.

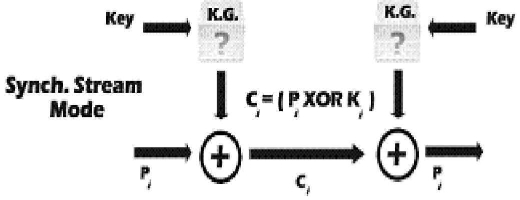


Figure6 Stream Cipher (Simple Mode)

Explanation

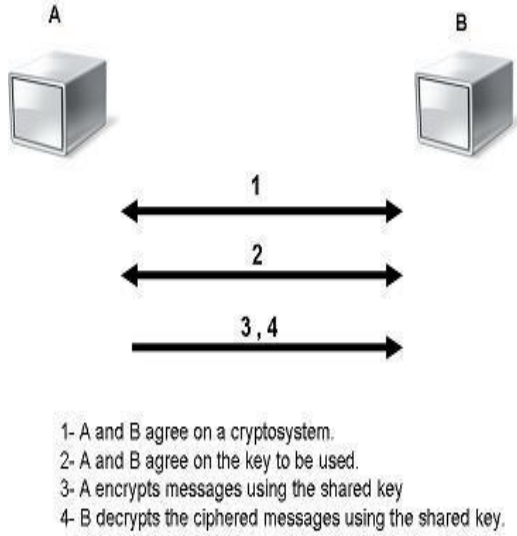
This section explains the two most common modes of operations in Block Cipher encryption-ECB and CBC- with a quick visit to other modes. There are many variances of block cipher, where different techniques are used to strengthen the security of the system. The most common methods are: ECB (Electronic Codebook Mode), CBC (Chain Block Chaining Mode), and OFB (Output Feedback Mode). ECB mode is the CBC mode uses the cipher block from the previous step of encryption in the current one, which forms a chain-like encryption process. OFB operates on plain text in away similar to stream cipher that will be described below, where the encryption key used in every step depends on the encryption key from the previous step. There are many other modes like CTR (counter), CFB (Cipher Feedback), or 3DES specific modes that are not discussed in this paper due to the fact that in this paper the main concentration will be on ECB and CBC modes.

- **Symmetric and Asymmetric encryptions**

Data encryption procedures are mainly categorized into two categories depending on the type of security keys used to encrypt/decrypt the secured data. These two categories are: Asymmetric and Symmetric encryption techniques

Symmetric Encryption

In this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages. Fig. 4 shows the process of symmetric cryptography. Node A and B first agree on the encryption technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection. After the encryption setup finishes, node A starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted messages.



1- A and B agree on a cryptosystem.
2- A and B agree on the key to be used.
3- A encrypts messages using the shared key
4- B decrypts the ciphered messages using the shared key.

Figure7 Symmetric Encryption

The main concern behind symmetric encryption is how to share the secret key securely between the two peers. If the key gets known for any reason, the whole system collapses. The key management for this type of encryption is troublesome, especially if a unique secret key is used for each peer-to-peer connection, then the total number of secret keys to be saved and managed for n-nodes will be n(n-1)/2.

For example, Let m be the plaintext message that Jude wants to secretly transmit to Kalu and let E_k be the encryption cipher, where k is a secret key. Jude must first transform the plaintext into ciphertext, c, in order to securely send the message to kalu.

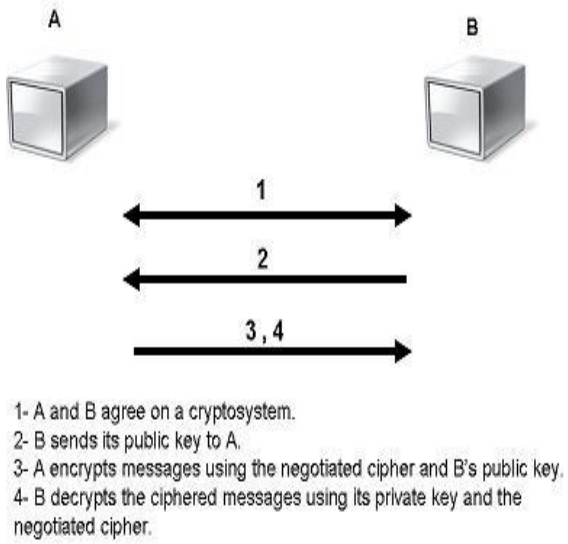
$c = E_k(m)$

Both Jude and Kalu must know the choice of key, k, or else the ciphertext is useless. Once the message is encrypted as ciphertext, Jude can safely transmit it to Kalu (assuming no one else knows the key). In order to read Judes's message, Kalu must decrypt the ciphertext using E_k^{-1} which is known as the decryption cipher, Dk.

$D_k(c) = D_k(E_k(m)) = m$

Asymmetric Encryption

Asymmetric encryption is the other type of encryption where two keys are used. To explain more, what Key1 can encrypt only Key2 can decrypt, and vice versa. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is known to the public, and private key which is known only to the user. Figure 5 below illustrates the use of the two keys between node A and node B. After agreeing on the type of encryption to be used in the connection, node B sends its public key to node A. Node A uses the received public key to encrypt its messages. Then when the encrypted messages arrive, node B uses its private key to decrypt them.



1- A and B agree on a cryptosystem.
2- B sends its public key to A.
3- A encrypts messages using the negotiated cipher and B's public key.
4- B decrypts the ciphered messages using its private key and the negotiated cipher.

Figure8 Asymmetric Encryption

This capability surmounts the symmetric encryption problem of managing secret keys. But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power. To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key, symmetric encryption is then used to transfer data between sender and receiver.

For example, in an open system, given any two principals X and Y, X should be able to encrypt a message that can only be decrypted by Y. If there is some binding established between principal identities and public keys, then these operations can easily be performed. A naive scheme might function as follows: principal X looks up public key K_Y for principal Y and uses it to compute an encryption for Y using some trapdoor function

$c = f_{KY}(m)$.

Then Y, on receipt of this message computes $f^1k_Y(c) = m$.

But there's a significant problem with this scheme given our definitions of security for shared-key encryption: it doesn't satisfy Semantic Security, since it's trivial for an adversary to compute $fK_Y(m)$ and $fK_Y(m')$ and compare them against given ciphertexts in the different attack models. Once again we see that there is no Semantic Security without probabilistic encryption. This is especially true in the public-key setting, since every principal has access to an encryption function for every other principal, by definition. Especially when the space of possible messages is small, it is easy to simply check all messages under the encryption function to figure out what has been encrypted.

- **Hybrid Encryption**

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure.

Method of Encryption Hybrid Encryption

- **Using Any Symmetric Algo And RSA Algo Encryption**

Steps using Hybrid Crypto System at the source Source: Has destination public key(PUK)

Inputs: Plain Data Block (PDB) Symmetric Key (SK)

Outputs: Encrypted Data Block (EDB)

Note: EDB contains both the encrypted PDB (denoted by ED) concatenated with encrypted SK (denoted by ESK)

Encryption Steps:

(1) Encrypt PDB using SK to get ED. (Note: This can be done using any symmetric-key crypto algorithm like DES and AES)

(2) Encrypt SK using destination's PUK to get ESK. (Note: This can be done using any public key algorithm like RSA)

(3) Concatenate ED with its corresponding ESK to get EDB which is sent to the destination.

EDB = { ESK , ED }

Decryption Steps using Hybrid Crypto System at the Destination Prerequisite:

Destination has its Private Key (PRK)

Inputs: Encrypted Data Block (EDB)

Note: EDB contains both the encrypted PDB (denoted by ED) concatenated with encrypted SK (denoted by ESK)

Outputs: Plain Data Block (PDB)

Decryption Steps:

(1) Decrypt ESK using PRK to retrieve SK.

Note: This should be done using the same public key algorithm which is used at source

(2) Use the retrieved SK as decryption key to decrypt ED to get PDB.

- **Hybrid Crypto System Using Rsa And D H**

Steps of this algorithm are as:

1. Choose two large prime numbers P and Q.

a. Calculate N = P x Q.

b. Select public key (i.e. encryption key) E such that it is not a factor of (p-1) and (q-1)

c. Select the private key (i.e. the decryption key) D such that the following equation is true

(D x E) mod (P – 1) x (Q – 1) = 1

Suppose R, S and G is automatic generated prime constants And put

A=E and B=D

2. Now calculate following as public number

X= GA mod R Y= GB mod R

3. Calculate session key with formula

KA = YA mod R KB = XB mod R

Such that KA = KB = K.

- **Hashing**

Hashing creates a unique, fixed-length signature for a message or data set. Each "hash" is unique to a specific message, so minor changes to that message would be easy to track. Once data is encrypted using hashing, it cannot be reversed or deciphered. Hashing, then, though not technically an encryption method as such, is still useful for proving data hasn't been tampered with. Here's a simple example:

Input Number

10,667

Hashing Algorithm

Input# x 143

Hash Value

1,525,381

You can see how hard it would be to determine that the value 1,525,381 came from the multiplication of 10,667 and 143. But if you knew that the multiplier was 143, then it would be very easy to calculate the value 10,667. Public-key encryption is actually much more complex than this example, but that's the basic idea. Public keys generally use complex algorithms and very large hash values for encrypting, including 40-bit or even 128-bit numbers. A 128-bit number has a possible 2^{128}, or 3,402,823,669,209,384,634,633,746,074,300,000,000,000,000,000,000,000,000,000,000,000,000 different combinations -- this would be like trying to find one particular grain of sand in the Sahara Desert.

VII. CONCLUSION

Security and integrity of data stored in cloud is a challenging task and of paramount importance to every organization using the system. Many research problems are yet to be identified. Cryptographic techniques are used to provide secure communication between the user and the cloud. Symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data in cloud storage. This paper proposed a symmetric encryption algorithm for secure storage of cloud user data in cloud storage. The proposed encryption algorithm is described in detail and the decryption process is reverse of the encryption. This algorithm is used in order to encrypt the data of the user in the cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication for the user. By applying this encryption algorithm, user ensures that the data is stored only on secured storage and it cannot be accessed by administrators or intruders.

REFERENCES

[1] Pardeep Sharma, Sandeep K. Sood, and Sumeet Kaur, "Security Issues in Cloud Computing", Springer-Verlag Berlin Heidelberg, HPAGC 2011, CCIS 169, pp 36–45, 2011.

[2] Vamsee Krishna, Yarlagadda And Sriram Ramanujam, "Data Security in Cloud Computing", Journal of Computer and Mathematical Sciences, Vol.2 (1), pp 15-23, 2011.

[3] Dr.A.Padmapriya, P.Subhasri," Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4, pp 1067-1071, 2013.

[4] Karen Scarfone, Murugiah Souppaya, Paul Hoffman, "Guide to Security for Full Virtualization Technologies ", http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125- final.pdf , NIST, 2011.

[5] Stratus Technologies, "white paper on Server Virtualization and CloudComputing:Four hidden impacts on uptime and availability" ,http://www.stratus.com/~/media/Stratus/Files/Library/WhitePapers /ServerVirtualizationandCloudComputing.pdf , 2011.

[6] Eman M.Mohamed, Hatem S.Abdelkader and Sherif El-Etriby, "Data Security Model for Cloud Computing", The Twelfth International Conference on Networks, ISBN: 978-1-61208-245-5, pp 66-74, 2013.

[7] Peter Mell, Tim Grance, "Effectively and Securely Using the Cloud Computing Paradigm", NIST, Information Technology Laboratory, http://www.csrc.nist.gov/groups/SNS/cloud-comput ing/cloudcomputing-v26.ppt. 2009.

[8] J.Srinivas, K.Venkata Subba Reddy and Dr. A.Moiz Qyser, "Cloud Computing Basics", International Journal of Advanced Research in Computer and Communication EngineeringVol.1, Issue 5, pp 343-347, 2012.

[9] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong, "The Characteristics of Cloud Computing", 39th International

[10] Tim Mather, Subra Kumaraswamy, and Shahed Latif "Cloud Security and Privacy", O"Reilly Media, Inc, pp 61-71, 2009. [10] Mohit Marwaha, Rajeev Bedi, "Applying Encryption Algorithm for

Data Security and Privacy in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, pp 367-370, 2013.

[11] V.U.K. Sastry, N. Ravi Shankar and S. Durga Bhavani, "A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration", International Journal of Network and Mobile Technologies, pp 45-53, 2010.

[12] Quist-Aphetsi Kester, "A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher", International Journal of Advanced Technology & Engineering Research (IJATER), Volume 3, Issue 1, pp 141-147, 2013.

AUTHORS

First Author – Okeke Stephen, Department of Computer Science, College of Physical and Applied Sciences, Michael Okpara University of Agriculture, Nigeria., okeke2020@yahoo.com, +2348133626900