Developing New Hybrid Cryptography Based Security for Cloud Computing System

[1] G.Narmadhai, [2]Dr. S. Vijay Bhanu
[1]Research Scholar, Department of Computer & Information Science, Annamalai University
[2]Assistant Professor, Department of Computer Science & Engineering, Annamalai University
[1,2]Annamalai Nagar – 608 002, India.

Abstract : In this age of cloud computing, we tend to store data which we need frequently in web based cloud storage services so that it can be accessed whenever we need them. This not only provides an immense amount of flexibility to users, but also makes our content accessible to us wherever we are and whenever we need them. We have many options in terms choosing web based cloud storage services for backing and archiving our data. There are many web based cloud storage services available out of which Amazon S3 and Google Drive are immensely popular among users. Backing up files so that they are not lost is an all-important step to ensure that nothing is ever lost. But, moving to the cloud is itself a big change and there are real concerns that make people pause before they sign up for any such service. This paper proposes and implements an algorithm which would encrypt the files uploaded on such web based cloud storage services and would decrypt the file once it has been downloaded using the keys that were generated during encryption. This would prevent unwanted intrusion into personal data and lack of standardization, i.e. one service provider may have end-to-end encryption while others do not.

IndexTerms **- Cloud Computing, Encryption, Decryption, Storage Devices;tting,style,styling,insert.**

I. INTRODUCTION

Imagine two people who share critical secret information have to split up. This requires them to share and communicate their data and information from a distance, even as there lays a threat of an eavesdropper having the ability to stop, interfere or intercept their communications and seeks that same information. They decide to lock their information in a box using a lock that only the other knows the combination to and has the key to open it. The box is locked and sent over to the other user who uses the combination key to unlock the box and read its contents. In simple terms, Cryptography [1] can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and are able to communicate information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is thus the science of making data and messages secure by converting the end user data to be sent into cryptic non-readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text [2] and then performing decryption which is reverting back to the original plain text. With this ability, Cryptography is used for providing the following security:

- Data Integrity: information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, its implementation for computer systems that store use data, processes, or retrieve that data.
- Authentication: for determining whether someone or something is, in fact, who or what it is declared to be.
- Non Repudiation: is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated.
- Confidentiality: relates to loss of privacy, unauthorized access to information and identity theft.

11

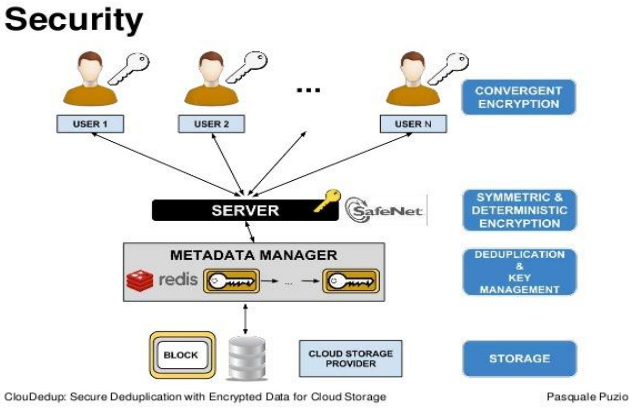

Fig 1: Encryption and Decryption process

In pure science terms [3], Cryptography is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and reconverting that cipher text back to plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cipher text. This can be interpreted as Cipher text C = E {P, Key} and Plain text C = D {C, Key}

Defining some terms used in Cryptography:

- Plaintext is the original intelligible source information or data that is input to algorithms
- Cipher text is the scrambled message output as random stream of unintelligible data
- Encryption Algorithm substitutes and performs permutations on plain text to cipher text
- Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text
- Keys are used as input for encryption or decryption and determines the transformation
- Sender and Recipients are persons who are communication and sharing the plaintext With respect to Cloud computing, the security concerns [4] are end user data security, network traffic, file systems, and host machine security which cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing. There are various security issues that arise in the Cloud:
- Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.
- Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet.
- Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
- Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service provider.
- User Access Control: for web based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers.

Security Algorithms are classified broadly as:

- Private Key / Symmetric Algorithms: Use single secret key are used for encrypting large amount of data and are have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, 3DES are some prime examples of this algorithms.

- Public Key / Asymmetric Algorithms: Use a key pair for cryptographic process, with public key for encryption and private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie Hellman are some types of public key algorithms.
- Signature Algorithms: Used to sign and authenticate use data are single key based. Examples include: RSA, DH
- Hash Algorithms: Compress data for signing to standard fixed size. Examples include: MD5, SHA

Some other ways of classifying Algorithms based on their processing features as below :With several Cloud services, Servers and hosted applications under IT management, most Cloud providers have no defined process to ensure security of data from threats and attacks [5]. Cyber attack these target the end user data for which the Cloud Service providers seek to try and secure by using Cryptographic algorithms whose primary goal is to make it as difficult as possible to ensure decrypting the generated cipher text from the plain text. When the key length is long, that makes it harder to decrypt the cipher texts, which in turn make the algorithms efficient and effective.

II. CLOUD COMPUTING PLATFORM

AbiCloud Platform: AbiCloud computing platform is designed, developed by Abiquo; an established cloud computing company in Barcelona Spain specialized in development of cloud platform. Peng, et al, (2009), state that Abicloud computing innovation can be used to building, managing as well as integration in a homogenous environment a private and public cloud virtualized infrastructure. Moreover, the platform can enable user's automatically and easily scaling, orchestration, deployment of variety of cloud utilities, including management of storage system, servers, virtual devices, networks and application.

Eucalypus: The Eucalyptus (Elastic Utility Computing Architecture for Linking Your Program to Useful Systems). Eucalyptus program conceptually commenced in California University Santa Babara, specifically as an open source used to build private cloud platform. Currently, it has transformed and run by a Eucalyptus company.

Nimbus: Nimbus cloud platform is an integrated open set tool, used to deliver, providing infrastructure as a service cloud computing solution supported by University of Florida and Chicago (Zeng et al., 2012). Nimbus platform is specifically designed based on science community interest such as batch schedulers, proxy credentials and best efforts allocation etc., although it have recently supported non scientific applications. It enables users to provide, build various remote computing on demand resources via deployment of virtual machines. Nimbus permits combination of Amazon, OpenStack and many other clouds.

Aneka Architecture: Aneka is a platform and a framework for developing distributed applications on the Cloud. It harnesses the spare CPU cycles of a heterogeneous network of desktop PCs and servers or datacenters on demand. Aneka provides developers with a rich set of APIs for transparently exploiting such resources and expressing the business logic of applications by using the preferred programming abstractions. System administrators can leverage on a collection of tools to monitor and control the deployed infrastructure. This can be a public cloud available to anyone through the Internet, or a private cloud constituted by a set of nodes with restricted access. Aneka is based on the .NET framework and this is what makes it unique from a technology point of view as opposed to the widely available Java based solutions.

III. RELATED WORKS

Zhiguo Wan, Jun'e Liu, and Robert H. Deng (2012) [6] proposed the technique HASBE (Hierarchical Attribute-set-based Encryption).HASBE extends the ciphertext-policy attribute-set-based encryption (CP-ASBE, or ASBE for short) scheme by Bobbaet al. with a hierarchical structure of system users, so as to achieve scalable, flexiblem and fine-grained access control.

Cong Wang Sherman S.M. Chow, Qian Wang (2013) [8] presents our public auditing scheme which provides a complete outsourcing solution of data—not only the data itself, but also its integrity checking. Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance.

Dijiang Huang (2015) [7] has discussed access control using Constant-size Ciphertext Policy Comparative Attribute- Based Encryption. CCP-CABE achieves the efficiency because it generates constant-size keys and ciphertext regardless of the number of involved attributes, and it also keeps the computation cost constant on lightweight mobile devices.

Jianan Hong(2015) [10] proposed that Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most attractive cryptographic techniques for data access control in cloud storage system, because of its fine-grained data access control policy and direct control of data for data owners. In CP-ABE, the user can access the content of the ciphertext, only if his/her attributes satisfy the ciphertext's preset access policy.

JieXu, Qiaoyan Wen, Wenmin Li and Zhengping Jin(2015) [9] were proposed Circuit Ciphertext-policy Attributeased Hybrid Encryption with Verifiable Delegation in Cloud Computing to keep data private and achieve access control. The anti-collusion circuit CP-ABE construction is used in this paper because CPABE is conceptually closer to the traditional access control methods.

Cloud computing is an upcoming paradigm that offers tremendous advantages in terms of economics, such as reduced time to market, flexible computing capabilities and limitless computing power. To use the full potential of cloud computing, data are transferred, processed and stored by external cloud providers. However, data owners are very sceptical of placing their data outside their own control sphere (Mithila and Kumar, 2011). The proposed solutions for network security include such concepts as cryptography whereupon the distribution of keys is done. Encryption and key generation are a vital tool for preventing threats to data sharing and preserving data integrity, so we are focusing on enhancing security by enhancing the level of encryption in the network. In their research,

Kuppuswamy and Al-Khalidi (2012) proposed selecting any number and calculating the inverse of the selected integer by using modular. This paper aims to propose an efficient method for providing data-storage security in cloud computing using the RSA algorithm. This algorithm includes some important security services such as key generation, encryption and decryption as they are provided in a cloud computing system (Sunitha and Prashanth, 2013).

The main scope of this paper is to solve security issues facing both cloud providers and cloud consumers using cryptography encryption methods. Understanding a cipher text is complicated compared to other methods (Subhasri and Padmapriya, 2013).

Singla and Singh (2013) described the cloud as being the most vulnerable next-generation architecture consisting of two major design elements: the Cloud Service Provider (CSP) and the client. Even though cloud computing is promising and efficient; there are many challenges in terms of data privacy and security. This paper explores the security of data at rest, as well as the security of data while moving (Subhasri and Padmapriya, 2013). Furthermore, Chavan and Bangare (2013) discussed a Customer Relational Management (CRM) system, a service using the RC5 algorithm, which is a block cipher notable for its simplicity, designed by Ronald Rivest in 1994; RC stands for "Rivest Cipher," or, alternatively, "Ron's Code" (Chavan and Bangare, 2013; Kuppuswamy and Al-Khalidi, 2012). In the proposed system, the party using cloud storage services must encrypt the data before sending it to the cloud while the service provider responsible for the encryption/decryption of the user's data must then delete the data once the encryption/decryption process is completed.

IV. PROBLEM STATEMENT

Cloud computing security is a very critical issue, where data can be in different physical locations at any data centre across the world network. This new technology structure leads to serious issues regarding security, such as authentication, data integrity, account or service hijacking, hypervisor vulnerabilities, data loss or leakage and confidentiality (Suthar, et al., 2012). In addition, the Cloud Security Alliance (CSA) (2013) identified data breaches as one of the top nine cloud computing threats for the year 2013, wherein a hacker is able to use sidechannel timing information to extract private cryptographic keys in use by other VMs on the same server. Despite this knowledge, it is not clear today how to coordinate appropriate and efficient incident responses without impacting the continuity of operations for other customers or without violating laws and contractual agreements. In addition, the speed with which incidents must be resolved becomes much greater. Since researchers of cloud computing security are giving less attention to selecting and using the right encryption and encoding algorithms, this paper proposes implementing secure developed security algorithms that could provide cloud storage higher performance and security as a replacement for the existing private cloud storage system.

V. EXISTING TECHNIQUES

Google Drive is a service that lets us store personal files on the cloud. Google Drive encrypts data using TLS (Transport Layer Security) standard even before it leaves the device. It is then uploaded to the drive. When the data reaches Google it is unencrypted and then re encrypted using 256-bit AES (Advanced Encryption Standard). The AES encryption keys used to encrypt the data are further encrypted with rotating master keys which adds a extra second layer of security, thus making the data more secure [5][17]. This process is simply reversed when we get data from Google Drive. Cloud Storage also allows us to enable versioning using which a history of modification and changes of all objects is kept in the bucket [18]. Amazon S3 stores objects redundantly across multiple facility in an Amazon S3 region. This redundancy helps is repairing data if there is a data corruption issue. In addition Amazon S3 also uses versioning to preserve every version of every object stored in our Amazon S3 bucket. Versioning allows us to easily recover from unintended user actions and application failures [6]. The server side encryption used by Amazon while the data is at rest i.e. stored in disks at Amazon S3 data centres, is similar to that to that of Google and it uses 256-bit AES to encrypt the data [20].

Although most of the service providers maintain high standards of encryption but encrypting data while when it is moved internally i.e. between the service providers own data centres and also encrypting data in transit i.e. while the data moves to and from the service providers remains an issue. Also, there exists lack of standardization, i.e. one service provider may have end-to-end encryption while others do not [7]. Currently lack of resources/expertise is the number one cloud challenge (as of 2016) but security is the second most important concern when it comes to the cloud [29].

VI. PROPOSED SOLUTION

The use of RC5 algorithm for encryption, cloud computing can be applied to the data transmission security. Transmission of data will be encrypted, even if the data is stolen, there is no corresponding key cannot be restored. Only the user knows the key, the clouds do not know the key. Also, because the properties of encryption, the cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage.

VII. RESULT ANALYSIS

Here we are comparing the actual result with Amazon s3 storage service. Amazon S3 (Simple Storage Service) is an online storage web service offered by Amazon Web Services. Amazon S3 provides storage through web services interface rest. Amazon S3 service graph. Fig. 6

Table 1.1: Comparison of Different Cloud services with Hybrid Encryption Algorithms

Tools	CPU Power		Memory	
	Available	Usage	Available	Usage
Amazon S3	100%	92.0%	82.0%	51.2%
Aneka 2.0	100%	98.4%	78.6%	78.4%
Nimbus	100%	97.5%	87.4%	64.5%
Eucalypus	100%	92.4%	83.6%	59.8%
AbiCloud	100%	95.8%	91.2%	71.7%

Advantages: - It provides strong security from the attackers. - But as the years passed by it was prone to a few attacks which were lesser when compared to DES, till date the only attack on it was Brute Force attack.

VIII. RESULTS AND CONCLUSION

In this paper we have proposed and implemented a symmetric key encryption algorithm to encrypt data at client side before uploading it to a cloud storage service. The main aim of this paper was to propose and implement an algorithm so that data can be encrypted at client side before it is uploaded to a cloud storage service because it provides an extra layer of security, minimises data theft in transit, minimises data intrusion and spying when data in moving within data centres of the service provider and also solves the problem of lack of standardisation,where some service providers guarantee end-to-end security but in reality their services are not secure. Hackers often trick a cloud into treating their illegal activity as a valid activity, and gain unauthorized access to the information stored in the cloud. This algorithm has been currently tested for text files especially, for which the encryption and decryption processes worked as expected. But, it could be further enhanced for encrypting other file formats or even audio and video files and even larger files could be encrypted at client side before uploading to the cloud.

IX. REFERENCES

[1] A Brief History of Cryptography, an article available at https://access.redhat.com/ blogs/ 766093/ posts/ 1976023, March 2016.
[2] Advances in Cryptography by Dara Kirschenbaum, History of Mathematics, Rutgers, Spring 2000.
[3] The Art Of Cryptology: From Ancient Number System to Strange Number System by Debasis Das, U.A. Lanjewar, S.J. Sharma, International Journal of Application or Innovation in Engineering and Management, Volume 2, Issue 4, April 2013.

[4] Cloud Computing – Understanding Risk, Threats, Vulnerability and Controls: A Survey, Manish M. Potey,C A Dhote, Deepak H. Sharma, International Journal of Computer Applications, Volume 67– No.3, April 2013.
[5] Encryption At Rest In Google Cloud Platform, an article available at https://cloud.google.com/security/encryption-at-rest/default-encryption/ , April 2017.
[6] Protecting Data Using Encryption, an article available at http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingEncryption.html .
[7] Top Ten Major Risks Associated With Cloud Storage, an article available at https://www.cloudwards.net/top-ten-major-risks-associated-with-cloud-storage/ , August 2015.
[8] Introduction to Cryptography, Principles and Applications by Delfs, Hans, Knebl and Helmut.
[9] Foundations of Security by Neil Daswani, Christoph Kern and Anita Kesavan.
[10] What is Amazon S3 ? , an article available at http://docs.aws.amazon.com/AmazonS3/latest/dev/Welcome.html .
[11] Working With Amazon S3 Buckets, an article available at http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingBucket.html .
[12] Top 10 Security Concerns for Cloud-Based Services an article by Joy Ma available at https://www.incapsula.com/blog/top-10-cloud-security-concerns.html , December,2015.
[13] A Short History Of Cryptography, an article by Fred Cohen.
[14] Past, Present, and Future Methods Of Cryptography And Data Encryption, A Research Review by Nicholas G. McDonald, Department of Electrical and Computer Engineering, University of Utah.
[15] Creating, Listing and Deleting Amazon S3 Buckets, an article available at http://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/examples-s3-buckets.html.
[16] What are the 12 biggest cloud computing security threats? , an article by Matthew Wilson available at https://www.ibm.com/blogs/cloud-computing/2016/04/12-biggest-cloud-computing-security-threats/ , April 2016.
[17] Managing Data Encryption, an article available at https://cloud.google.com/storage/docs/encryption#rotating-keys , January 2017.
[18] Object Versioning, an article available at https://cloud.google.com/storage/docs/object-versioning , April 2017 .
[19] An Evaluation of Amazon's Grid Computing Services: EC2, S3 and SQS by Simson L. Garfinkel, Computer Science Group, Harvard University, Cambridge, Massachusetts.
[20] Protecting Data Using Server-Side Encryption with Amazon S3-Managed Encryption Keys , an article available at http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html .
[21] AWS Regions and Endpoints , an article available at http://docs.aws.amazon.com/general/latest/gr/rande.html .
[22] Security Threats On Cloud Computing Vulnerabilities by Te-Shun Chou , Department of Technology Systems, East Carolina University, Greenville, NC, U.S.A , International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013 .
[23] An analysis of security issues for cloud computing by Keiko Hashizume , David G. Rosado , Eduardo Fernandez-Medina , Eduardo B Fernandez , Journal of Internet Services and Applications,2013 .
[24] The Cryptography, an article available at http://www.divini.net/tlm3/products0708/mathspedia/it/cryptography.pdf .
[25] Cryptography / History , an article available at https://www.saylor.org/site/wp-content/uploads/2011/03/History.pdf
[26] Study on symmetric key encryption: An Overview by Dharitri Talukdar, International Journal of Applied Research 2015 .
[27] Advances and Trends in Cryptography an article by Dr. Tomislav Nad , SIGS Technology Summit , June 2015 .
[28] An Overview of Cryptography an article by Gary C. Kessler, Embry-Riddle Aeronautical University - Daytona Beach, March 2016 .
[29] Cloud Computing Challenges Businesses are Facing These Days an article by Mona Lebied in Business Intelligence , January 2017.