ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Efficient Unflaws of Private and Public Verification Using ID-DPDP in Multi Cloud Storage

Pradeepa .S M.SC [1], Vijayalakshmi .K M.SC., MPHIL.,[1,2]

M. Phil Scholar, Dept. of Computer Science, Arignar Anna Govt Arts College, Cheyyar, India[1]

Assistant Professor, Dept. of Computer Science, Arignar Anna Govt Arts College, Cheyyar, India[2]

ABSTRACT: In Current world situation in involved many type of attacker to steal your own data for purpose of money and revenge. Cloud computing has important thing in computer field. Cloud computing takes information processing such as storage and computing .Data integrity verification is important thing in Cloud storage. In certain situation client should be store their own details such as image or text in multi cloud storage. The client stores own details in multi cloud servers, the distributed storage and integrity verification is very important. we purpose two model: novel remote data integrity checking model ID-DPDP(identity-based data provable data possession in multi cloud storage).formal system and security model Base64 and MD5.ID- DPDP is provable secure under the hardness assumption of standard CDH(computational Diffie-Hellman).ID-DPDP protocol can realize many verification delegated, private and public. Is an efficient and flexible in integrity verification.

KEYWORDS:ID-DPDP,CDH, BASE64,MD5 etc….

I.INTRODUCTION

1.1 NETWORK SECURITY :

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system.[11] An example of network security is an anti virus system.

A Model for Network Security

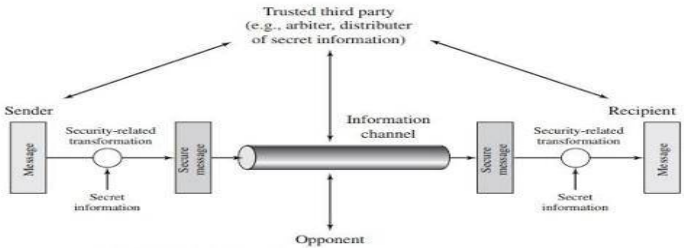


Fig 1.1

1.2 COMPUTER SECURITY:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

1.3 CRYPTOGRAPHY:

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. [11]Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Three types of cryptographic techniques used in general

1. Symmetric-key cryptography
2. Hash functions
3. Public-key cryptography.

The art of protecting information by transforming it (encrypt it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

BASE64 ALGORITHM:

Base64 is an algorithm that uses a concept of modern encryption algorithms [14]. It is a block cipher algorithm that operates on a bit, but the Base64 mode is easier in its implementation than others. Base64 is a general term for some similar encoding scheme that encodes binary data and translates it into a representation of the base 64. The term comes from the Base64 MIME encoding specific content. The base64 encoding scheme is typically used when there is a need to encode binary data.that needs to be stored and transferred through media designed to deal with textual data. This is to ensure that the data remains intact without modification during shipping.

a)Base64 encoding:

Base64 is a group of similar binary-to-text encoding schemes that representbinary data in an ASCII stringformat by translating it into a radix-64 representation .[14]The term Base64 originates from a specific MIME content transfer encoding.Base64 encoding schemes are commonly used when a need to encode binary data that needs to be stored and transferred over media that are designed to deal with textual data. This is to ensure that the data remains intact without modification during transport.

b)Base64 Decoding:

We will now tackle translating from base64 characters back into normal bytes[14]. We will use the same mapping of values (0 through 63) to base64 characters (A-Z, a-z, 0-9, '+', and '/'). We will now tackle translating from base64 characters back into normal bytes. We will use the same mapping of values (0 through 63) to base64 characters (A-Z, a-z, 0-9, '+', and '/'). The reverse process is relatively simple now that we know how to perform the forward operation. Let's start with the base64 string "YmFzZTY0IGlzIGZ1biEh". Right now, that makes no sense. We begin the same way, by looking up the value for each base64 character.

It is very important to remember that when you are encoding, you use 8 bits for each character, and when you are decoding you use 6 bits for each character.

II.LITERATURE REVIEW

2 .Dynamic block generation:

Admin configure MultiCloud server setup. Server IP Address and Port number is given by the admin for each Cloud. [1][2][3][4]Now a Server Architecture is created for MultiCloud Storage. If the admin has to reconfigure the old Multi Cloud server setup, it can be done. For old server setup, FAT file can be modified or remain same. Audit time will be set by the admin for Data Integrity checking process. The users provide their own personal information for this process. The server in turn stores the information in its database. After Registration, user can upload files to the server.Uploaded files will be stored in a Server. When the user upload the data to different cloud by the time it is Splitted into different blocks using Dynamic block generation Algorithm and each block will be appended with

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Signatures before Storing the data in FATFS. Signature generated using MD5 Algorithm. Also the data gets encoded using for Base64 Algorithm.

III. STRING MATCHING

String matching also known as pattern matching is one of primary concept for network security. In this area the effectiveness and efficiency of string matching algorithms is important for applications in network security such as network intrusion detection, virus detection, and signature matching and web content filtering system.[5] [6][7]A string matching technique is used for internet security purpose. Using filtering techniques, one can block various applications which you do not want to perform. This technique applies string matching process.

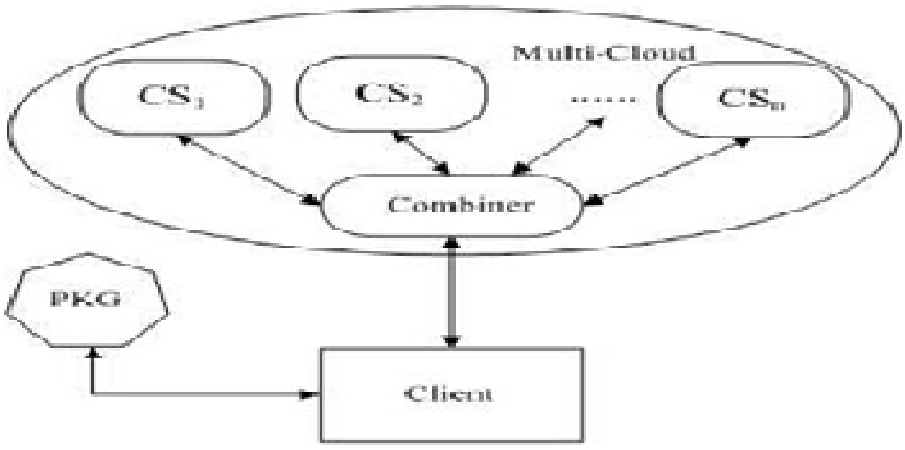
IV.VERIFIABLE DATA INTEGRITY CHECKING

Verifier performs Remote Integrity Checking on Cloud Data. Cloud allocates random combination of all the blocks to the Verifier, instead of the whole file is retrieved during integrity checking. This is to protect user privacy from a third party (Verifier). Verifiable Data Integrity Checking Algorithm is done in two steps: Block Checking and File Checking. In Block Checking step: Three signatures are generated for Block level Checking.

1. A signature of a block retrieved from a FATFS
2. A new signature is generated for block to be checked.
3. A Signature is retrieved from the block appended with the signature which is stored in the Cloud

The above three signatures are cross checked for Block level Integrity Checking. And the block contents are appended to verify with File level Integrity Checking.

Fig 4.1(ID-DPDP architecture)



V. MESSAGE DIGEST (MD5)

Message digest algorithm is a widely used cryptographic hash function with a 128 bit hash value[15].md5 has been employed is a wide variety of security applications and is also commonly used to check the integrity of files. However, it has been shown that Md5 is not on collision resistant;

MD5 algorithm can be used as a digital signature mechanism. This presentation will explore the technical aspects of the MD5 algorithm

Takes as input a message of arbitrary length and produces as output a 128 bit “fingerprint” or “message digest” of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

digest. Intended where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as PGP.

5.1. Md5 Algorithm:

MD5 is a message digest algorithm developed by Ron Rivest.

The original message digest algorithm is md; md5 is his fifth algorithm.It is fast produces 128 bit message digests. it can defined itself against collision.

MD5 algorithm that is used to verify data integrity through the creation of a 128 bit message digest from data input message of any length that is claimed to be as unique so that specific data as a finger print is specific to the individual. It is used with digital signature applications.

Which requires large files to be compressed by a secure method before encrypted with a secret key, under a public key cryptosystem original data undergo hashing operation to produce message digest (hash).

5.3 working of MD5:

Md5 process a variable length message into a fixed length output of 128 bits the input message is broken up into chunks of 512 bit blocks (sixteen 32-bit little endanin integers);the message is padded so that its lengthis divisible by 512.

Step1:Padding(adding)

 Adds padding bits to original message. It produce length of original message with padding bits, which is 64 bits less than an exact multiple of 512.

Step2: Append length:

The original message consisted of 1000 bits ,and we added a padding of 472 bits to make the length of the message 64 bits less than 1536(a multiple of 512 bits) the length is considered as 1000 and not 1472 for the purpose of this step. If length of messages exceeds 64 bits then only last 64 bits of length are used.

Step3: Divide the input into 512 bit blocks:

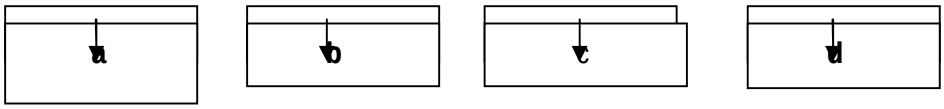
The input of the messages is now divided into blocks each of length is 512 bits .these blocks become input to the message digest processing logic

Step4: Initialize chaining variables:

Five chaining variables A through E is initialized in the case of SHA, we want to produce message digest of length 160 bits.

Step5: Process Blocks:

Copy four chaining variables into four corresponding variables a,b ,c,d



VI.ADVANTAGES AND DISADVANTAGES

The various advantages of MD5:

- Fast computation.
- Collision resistance.
- Is in widespread use.
- Provides a one-way hash.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

The various disadvantages of MD5:

- Has known security flaws and vulnerabilities.
- Is less securing then the SHA-1 algorithm.

VII. CONCLUSION

The two techniques are very useful to solve and secure the client own details from hackers. In multi cloud storage this paper formalizes the ID-DPDP system and security model. ID-DPDP protocol works flexibility and efficiently in multi cloud environment. At the same time ID-DPDP protocol can realize verification based on client 'authorization the first ID-DPDP protocol is provably securing under the assumption that the CDH is very hard.Base64 and MD5 is very securing the client information and much more efficiency and flexibility.

REFERENCES

[1] . C.C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, „„Dynamic Provable Data Possession,"" in Proc. CCS, 2009, pp. 213-222.
[2]. F. Sebe´, J. Domingo-Ferrer, A. Martı´nez-Balleste´, Y. Deswarte, and J. Quisquater, „„Efficient Remote Data Integrity Checking in Critical Information Infrastructures,"" IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.
[3]. H.Q.Wang. (2013, Oct./Dec.). Proxy Provable Data Possession in Public Clouds. IEEE Trans. Serv. Comput. [Online]. 6(4), pp. 551- 559. Available: http://doi.ieeecomputersociety.org/10.1109/ TSC.2012.35. [4]. Y. Zhu, H. Hu, G.J. Ahn, andM. Yu, „„Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage,"" IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244, Dec. 2012.
[5]. Y. Zhu, H.Wang, Z. Hu, G.J. Ahn, H. Hu, and S.S. Yau, „„Efficient Provable Data Possession for Hybrid Clouds,"" in Proc. CCS, 2010, pp. 756-758.
[6]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, „„MR-PDP: Multiple- Replica Provable Data Possession,"" in Proc. ICDCS, 2008, pp. 411-420.
[7]. A.F. Barsoum, and M.A. Hasan, Provable possession and replication of data over cloud servers", CACR, University Waterloo, Waterloo, ON, Canada, Rep. 2010/32. [Online]. Available: http://www.cacr.math.uwaterloo.ca/ techreports/2010/cacr2010-32.pdf.
[8]. Z. Hao and N. Yu, „„A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability,"" in Proc. 2nd Int. Symp. Data, Privacy, E- Comm., 2010, pp. 84-89.
[9]. A.F. Barsoum and M.A. Hasan, „„On verifying dynamic multiple data copies over cloud servers,"" Int. Assoc. Cryptol. Res., New York, NY, USA, IACR eprint Rep. 447, 2011. [Online]. Available: http://eprint.iacr.org/2011/447.pdf.
[10]. A. Juels and B.S. Kaliski, Jr., „„PORs: Proofs of Retrievability for Large Files,"" in Proc. CCS, 2007, pp. 584-597. [13] H. Shacham and B. Waters, „„Compact Proofs of Retrievability,"" in Proc. ASIACRYPT, vol. 5350, LNCS, 2008, pp. 90-107.
[11]. www.cs.columbia.edu/~hgs/teaching/security/slides/crypto2.pdf.
[12] http://www.webopedia.com/TERM/C/cryptography.html
[13]. www.idc-. online.com/technical_references/.../A_Model_for_Network_Security.pdf
[14]http://www.aardwulf.com/tutor/base64/base64.html [15]http://www.en.wikipedia.org/wiki/MD5