Data Integrity Inspection based on Modified Vernam Cipher Technique

[#1] V. Hema
Research Scholar
Bharathiar University,
Coimbatore

[#2] Dr. M. Ganaga Durga
Research Supervisor,
Bharathiar University, Coimbatore.
Asst. Prof. Department of CS,
Govt. arts College for Women, Sivagangai.

***Abstract*— Cloud Computing, evolving as a new system, makes adjustment for the exploitation of available resources that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLA) established through negotiation between the service provider and consumers [11]. One of the significant concerns that need to be addressed is to assure the integrity of the data stored in the archive. So, this paper offers Proof of Retrievability approach, called modified Vernam cipher, designed for data integrity verification in the cloud storage which leverages Cloud users from the security burden, by trusting a Third Party. This scheme which prevents the Cloud storage from modifying the data stored at it without the consent of the data owner. Based on theoretical analysis, we demonstrate that the proposed protocol has a provably safe and highly skilful data integrity checking measure**

Keywords*— *Cloud Computing, Data Integrity, Service Level Agreements, Cloud Archive, Third Party Auditor

I. INTRODUCTION

Computing is being transmuted to an archetypal consisting of services that are commoditized and provided in a manner similar to traditional utilities. The term “cloud “denotes the infrastructure from which businesses and users are able to access applications from anywhere in the world on demand. Thus, the computing world is rapidly transforming towards developing software, utilities etc. for millions to consume as a service, rather than to run on their individual computers. It rapidly provisioned and released the resources with minimal management effort or service provider interaction.

Cloud computing is a pioneering model, which benefit the user to utilize the on-demand high quality applications and services from a shared pool of configurable computing resources. By outsourcing data, consumers can be comforted from the burden of local data storage and maintenance. However, the fact that the users has no longer have physical control of the possibly large size of outsourced data. This makes the data integrity protection in Cloud a very tough and potentially frightening task, especially for users with constrained computing resources and capabilities. Thus, the auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed.

The third-party audit (TPA) mechanism is important and indispensable for the protection of data security and the reliability of services. TPA is an ideal security architect in a cloud environment, required for launching secure interactions between cloud client and cloud server. The proposed paper evaluates cloud security by ascertaining exclusive security requirements and tries to present a viable solution that eradicates the potential threats. The proposed uses modified symmetrical stream vernam cipher used to ensure the integrity and confidentiality of involved data and communications. Widespread security and theoretical analysis shows the proposed schemes are provably secure and highly efficient.

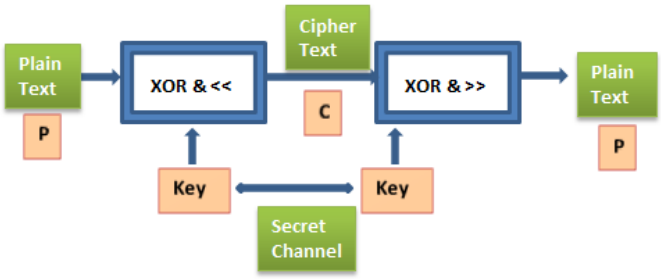
The rest of the paper is organized into 4 sections. Section 2 describes the concept of Modified Vernam Cipher. In Section 3, related data integrity works were reviewed. Section 4 illustrates the proposed system. Finally, Section 5 concludes the paper.

II. MODIFIED VERNAM CIPHER

Cryptography enables the user to store sensitive information or transmit it across insecure networks. So that it cannot be read by anyone except the intended recipient. A Vernam cipher is a symmetrical stream cipher in which the plaintext is combined with a random or pseudorandom stream of data of the same length, to generate the cipher text, using the Boolean "exclusive or" (XOR) function. Vernam cipher is defined as :

- Plaintext is a bitstring
- The secret key is a uniform distributed element of {0,1}
- The ciphertext is $C_{k.}$ (x)=(x $\oplus$ K) << 1

The cipher is reciprocal in that the identical keystream is used both to encipher plaintext to ciphertext and to decipher ciphertext to yield the original plaintext. If the keystream is truly random and used only once, this is effectively a one-time pad. Substituting pseudorandom data generated by a cryptographically secure pseudo-random number generator is a common and effective construction for a stream cipher [15]. The traditional vernam cipher is enhanced by adding bitwise shifting on both sides of transactions.



K- a long, non-repeating sequence of random numbers

Let m1 and m2 be encrypted under the same key k then,

$$c_1 = m_1 \oplus k$$

$$c_2 = m_2 \oplus k$$

then :

$$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2,$$

depends only on the plain text. Client needs the key to encrypt the plaintext; Server also needs the key to recover the plaintext from the cryptogram. An eavesdropper, who has intercepted the cryptogram and knows the general method of encryption but not the key, will not be able to infer anything useful about the original message. Indeed, Shannon proved that if the key is secret, the same length as the message, truly random, and never reused, then the one-time pad is unbreakable. Thus we do have unbreakable ciphers. The key should never be used more than once, because the attacker may subtract encrypted messages and get a combination of both unencrypted messages. The combined message can be decomposed to original messages using statistical methods.

III. RELATED WORKS

Cloud computing is a innovative and speedy growing technology that offers an pioneering and accessible solution for organizations to adopting various information technology resources such as software, hardware, network, storage etc. It is recognized as one of the most evolving technology. A momentous amount of research has been carried out to explore different areas in cloud computing. However, it also brings new challenges in creating secure and consistent data storage and access facility over insecure service providers. The integrity of data stored in the cloud storage is one of the challenges to be considered before the novel storage model is applied widely. Data Integrity proofs in cloud storage by Sravan Kumar provides a scheme for static storage of data [2] with bare minimum costs and less effort. To ensure confidentiality and integrity of the information, a truthful service based on trusted encryption scheme is provided with rigid access controls and scheduled data backups.

An improved method [4] for Proof of Retrievability is offered based on embedding crafted meta data into the original file F and verify its exactness. This scheme comes with partial encryption process. Juels described a formal "proof of Retrievability" model for confirming the remote data integrity. Their proposal combines spot-checking and error correcting code to make sure both the possession and retrievability of files on archive service systems.

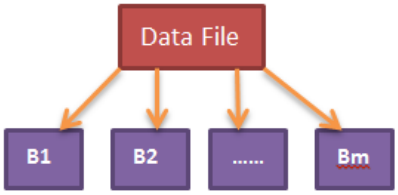
Merkle Hash Tree Technique [5] is also introduced for Authentication and integrity issues in cloud, However, all these schemes are focusing on the static data. A Traditional RSA algorithm [7] based scheme is introduced to maintain the integrity of the data storage, but it uses the tedious factorization process which slow down the encryption and decryption process. A challenge-response protocol [9] for dynamic data storage is designed to determine data correctness and also locate the possible local errors.

Shacham built a model based on random linear functions which enables unlimited number of queries and requires less communication overhead. Bowers proposed an improved framework for POR protocols that generalizes both Juels and Shacham's work. Later in their succeeding work, Bowers extended POR model to distributed systems. Another Proof of Retrievability approach is designed, which uses special blocks called "Sentinels", that are randomly embedded into the data file for the purpose of detecting the modification of the server data. An improved POR Scheme based on verifiable homomorphic authentication using BLS signatures is used to provide the proof for the data in the storage.

IV. PROPOSED SYSTEM

The objective of this paper is to present a remote data integrity checking protocol based on modified Vernam symmetrical stream cipher to guarantees not only correct data possession but it also assures retrievability upon some data corruptions, with the support of public auditability. Data security is of vital importance so that client can resort a provable Data Possession (PDP) Scheme, which uses the RSA cryptographic technique that allows the user to store their data at an untrusted server. This scheme has probabilistic guarantees that the server possesses the original data. Client encrypts the data file F using Number Theory based RSA algorithm, which is used to secure data while it is being transferred in and out of the cloud. In order to speed up the encryption process, tedious factorization process is replaced by Successive Squaring technique. Third party auditor sets the bounded query scheme with the server based on the service level agreement (SLA) and audits the cloud storage without demanding the local copy of data and does not produce burden to the user. Thus, cost complexity involved in integrity checking process is less compared to the existing protocol and also applicable for all kinds of cloud models.

Vernam stream cipher scheme is used for the verification of validity of data existing in archive. The File F' consists of n file blocks. Each block comprises m bits of data. The k bits of each block selected for crafting the meta data based on the modified vernam cipher scheme.



A data file F with m blocks

Fig 1. File with data blocks

For every block in the file f', craft the metadata using the keystream which is generated randomly using the *Random ( )* Function and *Bitwise shifting* operations. Finally append and upload the file F' into the storage archive. If the TPA wants to verify the integrity of the file F', it throws a challenge to the archive and gets a response to check the correctness of data. TPA generates and sends key stream to the server for challenge. Server based on the information given by the TPA, decode the data and send the response back to the server.

Working principle of the algorithm :

Consider the plain text (p) = "algo". Using the number theory based RSA algorithm, it is encrypted as C=59 04 38 45. The RKey (i.e) key stream is generated using the following code snippet:

```
Random t = new Random();
// random integers in [0, 100]
for (int c = 1; c <= 10; c++)
RKey(i)=(t.nextInt(100));
```

The metadata is generated using the following:

$$Metadata = (BE \oplus RKey) << 1$$

Table 1. Metadata Generation

Sno	characters	Decimal Encrypted	Bitgroup Encrypted (BE)	RKey	Bitgroup RKey	BE ⊕ RKey
1	a	59	00111011	62	00111110	00001010
2	l	04	00000100	47	00101111	01010110
3	g	38	00100110	60	00111100	00110100
4	o	45	00101101	17	00010001	01111000

All the meta data bit blocks are generated using the above procedure and appended to the file F' before storing it at the cloud archive. Server decodes the text using the bitwise right shifting and XOR function (i.e)

$$BS = (ciphertext) >> 1$$
$$Decimal\ encrypted = RKey \oplus BS$$

Table 2. Metadata Verification

Sno	RKey	Bitgroup RKey	Cipher Text	Bitwise shifting (BS)	RKey ⊕ BS	Decimal Encrypted
1	62	00111110	00001010	00000101	00111011	59
2	47	00101111	01010110	00101011	00000100	04
3	60	00111100	00110100	00011010	00100110	38
4	17	00010001	01111000	00111100	00101101	45

and send response to the client for their challenge made through TPA.

The challenge and the response are equated and if the outcome is true, the TPA accepts the validity and sends the status report to the client. Any mismatch between the two, would mean a loss of the integrity of the client data at the cloud storage. If the client want to modify or delete some block information in F' stored in the outsourced server, it send a stop signal to the TPA. TPA then halts checking and delays till the resume signal received from the client. The holder prepares block information, key information and location to insert/modify the block and sends these to the server. The server after receiving the appeal, append and update the data file F'. Then generate the metadata for newly created blocks in the F'. Owner then send resume signal and ask the TPA to prepare a metadata for the newly inserted block. This protocol is suitable for text content only. In further research process, image file is separated, check the validity using the suitable algorithm and concatenated into the original file F'.

CONCULSIONS

Cloud computing is now becoming a business standard. It simplifies the user's accessibility. It provides a virtual storage space to the user which could be used without bothering about the details of the entire mechanism. It offers a worthy number of paybacks for its users. However, it also nurtures some security plights which may slow down its fame. Vulnerabilities exist in cloud computing will be identified which helps the organizations to make the shift towards the cloud. The proposed paper assesses the cloud security by identifying the susceptibilities exist in cloud computing and attempt to present a viable solution that eliminates these potential threats. The symmetrical stream cipher based technique is used for checking the validity of data and the exactness of computations done by Server and TPA is proposed.

The protocol proposed is beneficial to the user because it reduces the burden at the client side. TPA is prompted to uphold the validity of the data in the file F' periodically. Through theoretical analysis, we demonstrate that the suggested protocol has very virtuous efficiency in the aspects of communication, computation and storage costs. Our goal is to present a better understanding of the relative merits of this protocol and provide a beneficial protocol for supporting the data integrity checking.

REFERENCES

[1] Catteddu, Daniele, and Giles Hogben. "Cloud computing risk assessment."European Network and Information Security Agency (ENISA) (2009).Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer Systems 28.3 (2012): 583-592.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[2] Sravan Kumar, R., and Ashutosh Saxena. "Data integrity proofs in cloud storage." Communication Systems and Networks (COMSNETS), 201.1.

[3] Kaufman, Lori M. "Data security in the world of cloud computing." Security & Privacy, IEEE 7.4 (2009): 61-64.
[4] Neha, T., and P. S. Murthy. "A Novel Approach to Data Integrity Proofs in Cloud Storage." International Journal 2.10 (2012).M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[5] Desale, Mrs Vrushali R., and Pradeep K. Deshmukh. "Multi Client Support Third Party Auditor (TPA) for Cloud Data Integrity and Security." International Journal3.6 (2013).
[6] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989. Ryan, Mark D. "Cloud computing security: The scientific challenge, and a survey of solutions." Journal of Systems and Software (2013).
[7] Kalpana, Parsi, and Sudha Singaraju. "Data Security in Cloud Computing using RSA Algorithm." IJRCCT 1.4 (2012): 143-146.
[8] Shinde, G. N., and H. S. Fadewar. "Faster RSA Algorithm for Decryption Using Chinese Remainder Theorem." ICCES: International Conference on Computational & Experimental Engineering and Sciences. Vol. 5. No. 4. 2008.
[9] Wang, Qian, et al. "Enabling public auditability and data dynamics for storage security in cloud computing." Parallel and Distributed Systems, IEEE Transactions on 22.5 (2011): 847-859..
[10] Luo, Wenjun, and Guojing Bai. "Ensuring the data integrity in cloud data storage." Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on. IEEE, 2011.
[11] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 25:599 616, 2009
[12] Hao, Zhuo, Sheng Zhong, and Nenghai Yu. "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability."Knowledge and Data Engineering, IEEE transactions on 23.9 (2011): 1432-1437.
[13] Popovic, Kresimir, and Zeljko Hocenski. "Cloud computing security issues and challenges." MIPRO, 2010 proceedings of the 33rd international convention. IEEE, 2010.
[14] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation Computer Systems 28.3 (2012): 583-592.
[15] Rogaway, Phillip, and Don Coppersmith. "A software-optimized encryption algorithm." Journal of Cryptology 11.4 (1998): 273-287.
[16] Zhang, Ya-Ping, Jizhou Sun, and Xu Zhang. "A stream cipher algorithm based on conventional encryption techniques." Electrical and Computer Engineering, 2004. Canadian Conference on. Vol. 2. IEEE, 2004.