International Journal of Computing Algorithm
Volume: 04 Issue: 01 June 2015 Pages:33-36
ISSN: 2278-2397

Effectual Data Integrity Checking Technique Based on Number Theory

V.Hema[1], M.GanagaDurga[2],G.Yogeswari[3]
[1]Research Scholar, Bharathiar University, Coimbatore
[2]Research Supervisor, Bharathiar University, Coimbatore, Assistant Professor, Department of CS,
Govt. Arts College for Women, Sivagangai,
[3]Software Engineer,Wiaan Business Corporation Software Lab,Karaikudi.
Email: vhema23@gmail.com, mgdurga@yahoo.com

Abstract-Cloud Computing makes data really mobile and a client can simply access a chosen cloud with any internet accessible device. The espousal and dispersion of Cloud computing are threatened by unresolved security issues that affect both the cloud provider and the cloud user. The integrity of data stored in the cloud is one of the challenges to be addressed before the novel storage model is applied widely. This paper analyses the efficiency issues and security dodge of an existing scheme and proposes an amended data integrity scheme using improved RSA and number theory based concept for cloud archive. This scheme of protecting the integrity of guest virtual machines can be agreed upon by both the cloud and the customer and can be incorporated in the service level agreement (SLA).Based onhypothetical analysis, we demonstrate that the proposedscheme has a provably safe and highly adroitdataintegrityinspection measure.

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

I. INTRODUCTION

Cloud computing reinforces the idea that computing and communication are deeply intertwined and provides vast amounts of computing cycles and storage space to be made availableto the on-demand user on a pay-as-you-go model.This has drawn a lot of attention towardsthe domain in recent years. Data Security is a crucial element that warrants scrutiny. The main unease around the data putting away is the protection of information from unauthorized access. Resources that sit outside the user's domain have the risk that, someone can access and corrupt data is considerable. Before the user move their data to the cloud, all issues deriving from storing data on outsourced servers and un-trusted resources must be addressed, including the inconsistencies with this new model, put there by the legal frameworks. Data outsourcing can release the user from the burden of local data storage. But the users have no longer had physical rheostat of the outsourced data. This makes the data integrity protection in cloud a very hard-hitting and potentially startling task, especially for users with constrained computing resources and capabilities. So, the proposed system provides a secure storage approach to avoid insider threats using improved RSAcryptosystem to protect the data from unauthorised access.

The main idea of this system is that the punter performs some pre-processing over the data before sending it to the entity in charge of the computation. This pre-processing adds some structured randomness. After the computation, some post-processing is required to remove the added randomness and reveal the final computation output.A third trusted party (TTP) is an ideal security builder ina cloud environment, required for hurlingsecure interactions between client and server. The proposed paper appraises security issues by ascertainingelite security requirements and presents adoable solutionfor guarding the integrity of guest virtual machines that can be performed using cryptographic technique and number theory based systems. The theoreticalanalysis and experimental results shows the proposed schemes are provably secureand highly efficient.The rest of the paper is organized into 4 sections.Section 2 describes the concept of Improved RSA cryptosystem using Short Range Natural Number(SRNN). Section 3, describes the concept of Residue Number System. Section 4, describes the concept of Chinese Remainder Theorem. In section 5, related data integrityworks were reviewed. Section 6 illustrates the proposedsystem. Section 7, illustrates the results of the proposed system. Finally, Section 8 concludes the paper.

II. IMPROVED RSA CRYPTOSYSTEM USING SHORT RANGE NATURALNUMBER(SRNN) ALGORITHM

A Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. Resources that sit outside the user's domain have risk that someone can access and divulge data. In this paper, we addressthe issuesand inconsistenciesderiving from storing data on un-trusted resources and provide the legal framework which guarantees the integrity of involved data and communication.This secure storage approach aims to avoid insider threats using improved RSA Cryptosystem using SRNN algorithm which securely perceive and authenticate implicated entities.he Short Range Natural Number (SRNN) algorithm uses two natural numbers in pair of keys which enhance the security of the cryptosystem. Because of increased security, it is well suited for multiuser environment.This system uses two random large prime numbers p and q of bit length equal to 1024 bytes. This random numbers p and q should not be repeated so we make use of two small natural numbers u and a for encryption and decryption processes. The Key Generation, Encryption and Decryption Process of the algorithm are given below:

A. Key Generation Process

- Generate two large random primes, p, q and their product n = p x q is of the required bit length, e.g. 1024 bits.
- Compute $\varphi = (p-1)(q-1)$.
- Choose an integer e, $1 < e < \varphi$, such that gcd $(e, \varphi) = 1$.
- Compute the secret exponent d, $1 < d < \varphi$, such that $(ed) \bmod \varphi = 1$.
- Select the short range natural number u, such that $u < \varphi - 1$.

International Journal of Computing Algorithm
Volume: 04 Issue: 01 June 2015 Pages:33-36
ISSN: 2278-2397

- Select the another short range natural number a randomly such that φ> a > u and also compute ua .
- calculate d such that, e * d mod ((p-1)*(q-1)) = 1
- The public key is (n,e,ua) & the private key is (d,a,u).

B. Encryption Process

- Obtains the recipient's public key (n,e,ua)
- Represents the plaintext message as a positive integer m.
- Computes the cipher text c = (m ua)e mod n.
- Sends the cipher text c to recipient.

C. Decryption Process

Uses his private key (d, a, u) to compute m = (v e c) d mod n Where v= u phi-a mod n.

- Extracts the plaintext from the integer representative m.

Using this fusion of two algorithms, we found that when modulus length increases, security increase and speed decrease.

III. RESIDUE NUMBER SYSTEM

Residue Number System (RNS) is a non-weighted and non-positional number system which can be represented completely by specifying its base and does not have a single fixed radix. Residue number systems provide a good means for extremely long integer arithmetic. Their carry-free operations make parallel implementations feasible. It is a valuable tool for theoretical studies of the limits of fast arithmetic integer system. RNS convert arithmetic on large numbers to arithmetic on small numbers. The RNS bases are represented by N-tuple of integers $\{m_1, m_2, \ldots m_n\}$ where each of these bases is called a modulus. The general form of RNS is :$x=q_i\ m_i + r_i$, *where* $i=1,2\ldots N$.

The residue representation is N-tuple $\{r_1, r_2, \ldots ,r_n\}$defined by a set of N equations. The quantity r_i is the least nonnegativeinteger remainder of the x/m_i designated as theresidue of $|x|_{mi.}$ The integer r_i is the i-th residue digitof x. Residue Number System applied on finite ring andthe moduli of the system have to be pair wise relativelyprime integers, (i.e.) no two modulus have a GCD greaterthan 1.A finite ring is a set of finiteelements over which modular addition and modularmultiplication operations are defined. Theresult of the system must exist within the ring definedby the system and the finite ring of the system has the elements {0, 1, 2, ..., M-1},whereM is a measure of dynamic range of the system and theinterval *[0, M-1]* is called the legitimate range of the RNS. The dynamicrange (M) of the system is *[-(M-1)/2,(M-1)/2,* if M is odd and *[-M/2, (M/2-1)]* , if M is even.Within this dynamic range, every number can berepresented by a unique set of residues$\{ r_1, r_2, \ldots ,r_n \}$, *where* $r_i = x \bmod m_{i.}$

The effective choice ofthe moduli guarantees the most efficient outcome. The three moduli set {2n–1, 2n, 2n+1} is of special interest because several operations in this system can be performed efficiently with limited amount or even without ROM.The periodicity properties exhibited by three moduli results in splendid performance of the binary to residue converter and modulo addition even for large numbers.

IV. CHINESE REMAINDER THEOREM

The Chinese Remainder Theorem (CRT) is the theorem that enables the conversion of residues back into decimal number. The residues$\{ r_1, r_2, \ldots ,r_n \}$ of a number X, can be converted back into X, provided the greatest common divisor ofany pair of moduli is 1. The theorem can also be generalized as follows. Given a set of simultaneous congruence's,$X \equiv a_i (mod\ m_i)$ fori= 1, 2…r, and for which the m_i are pairwise relatively prime, the solution of the set of congruences is

$X \equiv a_1 b_1 (M / m_1) + \ldots + a_r b_r (M / m_r)\ (mod\ M)$, where

M= $m_1\ m_{2\ldots\ldots} m_r$ *and the* b_i ,are determined from

$b_i (M / m_i) \equiv 1\ (mod\ m_i)$.

This Theorem is mainly used in the verification phase of the integrity checking process.

V. RELATED WORKS

Cloud computing is not just a concept technology that promises to deliver many electrifying things. Cloud computing is a subscription based service where user can obtain networked storage space and computer resources. Resource sharing is a pure plug and play model that dramatically simplifies infrastructure planning. However, it also brings new challenges in creating secure and consistent data storage and access facility over insecure service providers. To ensure confidentiality and integrity of theinformation, SravanKumar [2]provides a truthful service based on trustedencryption scheme with rigid access controlsand scheduled data backups.Bowers extended "proof of retrivabilty"(POR) model to distributed systems; all these schemes are focusing on static data. The effectiveness of their scheme rests mainly on the proposing steps that the user conducts before outsourcing the data file. Any change to the contents of data file,even few bits must propagate through the error-correcting code and thecorresponding random shuffling process,thusintroducing significant computation and communication complexity.

An improved method[13] for Proof of Retrievability is offered based onembedding crafted meta data into the original file F andverifies its exactness. This scheme comes with partialencryptionprocess.Juelsdescribesa"proof of Retrievability"model for confirming the remote data integrity. Theirproposal combines spot-checking and error correctingcode to make sure both the possession and retrievabilityof files on archive service systems. Merkle Hash Tree Technique [5] isalso introduced for Authentication and integrity issues incloud, However, all these schemes are focusing on thestatic data. A Traditional RSA algorithm [7] basedscheme is introduced to maintain the integrity of the datastorage, but it uses the tedious factorization processwhich 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.Erway et al. [11]were the first to explore constructions for dynamic provable data possession. They extend the PDP model to support provable updates to stored data files using rankbased authenticated skip lists.This scheme is essentially a fully dynamic version of the PDP solution. To support updates, especially for block insertion, they eliminate the index information in the "tag" computationinAteniese's PDP model

International Journal of Computing Algorithm
Volume: 04 Issue: 01 June 2015 Pages:33-36
ISSN: 2278-2397

and employ authenticated skip list data structure to authenticate the tag information of challenged or updated blocks first before the verification procedure. However, the efficiency of their scheme remains unclear

Shacham built a model based on random linearfunctions which enables unlimited number of queries andrequires less communication overhead. Bowers proposedan improved framework for POR protocols thatgeneralizes both Juels and Shacham's work. Later intheir succeeding work, Bowers extended POR model todistributed 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 holomorphic authentication using BLS signatures is used to provide the proof for the data in the storage.From the above studied schemes, we can say that, the existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting both public auditability and data dynamics has not been fully addressed. This paper aims to design a safe and effectual protocol to integrate these two import components for data storage archive.

VI. PROPOSED SYSTEM

Cloud computing involves frequent uploading and downloading of data in archive along with ample reckoning on servers which are managed by trusted third party. Since the client does not control the cloud environment.So, integrity checking becomes imperative to secure data in a cloud environment.It is very significant to use required cryptographic algorithms to save client data on cloud network.To provide data security, sensitive user data is encrypted usingRSAalgorithm fused with SRNN algorithm which guarantees not only correct data possession but also assures retrievabilitywith the support of public auditability. Also an improved POR scheme based on number theory is used to provide the proof for the data in the storage.The proposed work lures conceptual cloud architecture by espousing an encryption algorithm with dynamic key to ensure the security and doesn't compromise any information with the cloud server. TTPhas the capability to verify outsourced data periodically, helps the client to encrypt their information, partitioned into multiple segments based on the remaining dynamic storage capacity presents in the VMs of cloud storage servers, crafting metadata and store these encrypted segments of the clients' file on the corresponding VMs of the cloud storage providers. The following are the phases of Integrity checking process:

D. Meta Data Generation Phase

The basic initiative in this system is that, thedata file is divided into n blocks and each blocks has m bytes (i.e.)b_1, b_2... b_m. The client craft suitable metadata and encryptsthe n blocks which are used afterwardsin auditing process. In integrity checking scheme, Residue Number System and Chinese Remainder Theorem plays a vital role in generation and verification of Meta data. The meta data created using *MD=i+j*(c[i,j]+sum of residue),* is appendedto the file itself. Finally, upload the File F' to the storagearchive.For example,the metadata crafting for the text file F which contain the text "CLOUD", as follows.

E. Meta Data Verification Phase

To check the integrity of the file, the TTP send a challenge (i, j, residue set, moduli set) to the server. The server calculates the Meta data using the Chinese remainder theorem (CRT) and sends the cipher value to the TTP. TTP check the equality and send the status report to the client. For the challenge(1,1,{2,3,1},{3,4,5}), it compute the metadata as follows.

First it calculates the c(i,j) using the Chinese Reminder Theorem as :

M=m1xm2xm3, M=60 , M1=20, M2=15, M3=12
Inverse of M1,M2,M3=2,3,3

$$X = \left| \sum_{i=1}^{3} r_i \left| M_i^{-1} \right|_{m_i} M_i \right|_{60}$$

$X = \left| 2x20x2+3x15x3+1x12x3 \right|_{60}$
X=11 (i.e.) c(i,j)=11

Then it calculate the metadata using the *MD=i+j*(c[i,j]+sum of residue),* and send the value 132 to the TTP as a response.
If the TTP wants to corroborate the integrity of the data file *F',* it flings a challenge to the archive and gets a rejoinder to check the correctness of data. TTP engenders 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. 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.

Third party 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.The proposed design supports continued safe and efficient dynamic activities, including block modification, deletion and append with the help of TTP. This system is very effective against server colluding attacks and data modification attacks.TTP standstills checking and delays till the resume signal received from the client. The data owner prepares block information, key information and location and sends these to the server. The server after receiving the entreaty, append and update the data file F'. The metadata generation for newly created blocks are also performed by TTP. In further research process, image file is separated, check the validity using the suitable algorithm and concatenated into the original file F' A PDP technique used in this system provide high end security and the integrity audit of data in storage outsourcing

VII. RESULTS

Several secure integrity checking of outsourcing techniques have been proposed and there are archetypal results for the problems of secure two-party and multi-party computation. In most cases, the main inkling is that the owner performs some

International Journal of Computing Algorithm
Volume: 04 Issue: 01 June 2015 Pages:33-36
ISSN: 2278-2397

pre-processing over the input data before sending it to the archive in charge of the computation. This pre-processing adds some structured randomness. After the computation, some post-processing is required to remove the added randomness and reveal the final computation output.

Character	ASCII	Block(i)	Block(j)	C(i,j)	Residue Sum (RS)	Meta data(MD)
C	99	1	1	11	6	132
L	108	1	2	20	2	120
O	111	1	3	155	5	3100
U	117	1	4	161	4	3220
D	100	2	1	144	4	1728

The performance analysis is done on the basis of total execution time and speed-up ratio on varying input size. JAVASE-1.7 on Eclipse Luna and CloudSim is used for the development of the algorithm.We focus on the user friendly GUI mode implementation. Default values of input filename, encrypt filename, decrypt filename, key size, message block size, prime numbers (p,q), natural numbers are used and user have flexibility to change these values as and when required. SRNN cryptosystem make use of natural numbers,toprovideenhanced security algorithm.

Table 1 shows the comparison on the basis of recorded time

S.No	Modulus Length	Block size	RSA Algorithm				SRNN Algorithm			
			KG Time	ETime	DTime	Total Time	KG Time	ETime	DTime	Total Time
1	256	128	50	55	340	445	60	95	800	955
2	512	256	165	75	890	1130	178	110	2115	2403
3	1024	512	500	115	2658	3278	570	160	7200	7930

The Table 1 shows the general comparisons between RSA and RSA-SRNN algorithm. In this analysis, we found that when the modulus length increases and speed decreases. And also when the block size increases, both the security and speed increases. From the overall performance, we conclude that the RSA-SRNN is better in security but slower in speed. Hence the RSA-SRNN with modulus length 1024 bits is good balance between the speed and the security. In future, we planned to include Chinese Remainder Theorem(CRT) based RSA scheme[10] results in a decryption process which is much faster than Modular Exponentiation with the Average of 0.044 sec per decryption, giving Speedy original Data.The proposed design allows users to audit the cloud storage with very lightweight communication and computation costs.. This scheme ensures that the storage at the client side is minimal which will be beneficial for thin clients.

VIII. CONCLUSIONS

Cloud computing reflects the latest trends in business to deliver software and services over the Internet.It offers a worthy number of benefits for its users. 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 technique used for checking the validity of data and the exactness of computations done by Server and TPA is proposed. Through theoretical analysis& experimental results, we demonstrate that the suggested protocol has very virtuous efficiency in the aspects of communication, computation and storage costs. In future, we planned to provide a beneficial and high speed protocol for supporting the data integrity checking for multimedia.

REFERENCES

[1] Kaufman, Lori M. "Data security in the world of cloud computing." Security & Privacy, IEEE 7.4 (2009): 61-64.
[2] Sravan Kumar, R., and AshutoshSaxena. "Data integrity proofs in cloud storage." Communication Systems and Networks (COMSNETS), 201.1.
[3] Catteddu, Daniele, and Giles Hogben. "Cloud computing risk assessment."European Network and Information Security Agency (ENISA) (2009).Zissis, Dimitrios, and DimitriosLekkas. "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.
[4] Popovic, Kresimir, and ZeljkoHocenski. "Cloud computing security issues and challenges." MIPRO, 2010 proceedings of the 33rd international convention. IEEE, 2010.
[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 SudhaSingaraju. "Data Security in Cloud Computing using RSA Algorithm." IJRCCT 1.4 (2012): 143-146.
[8] Luo, Wenjun, and GuojingBai. "Ensuring the data integrity in cloud data storage." Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on. IEEE, 2011.
[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] 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.
[11] Erway, Chris, et al. "Dynamic provable data possession." Proceedings of the 16th ACM conference on Computer and communications security. ACM, 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] 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.
[14] Zissis, Dimitrios, and DimitriosLekkas. "Addressing cloud computing security issues." Future Generation Computer Systems 28.3 (2012): 583-592.
[15] 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