Amalgam Of Hamming Weight-Based RSA And Multi Party Computations To Enhance Security In Multi Cloud Ambience

Parsi Kalpana

***Abstract*: Cloud Computing, apparent technology has both advantages and disadvantages. In spite of multitudinous benefits Cloud is offering, broad acceptance of Cloud has taken a toll on the basic security in cloud environments. It becomes more pronounced when thinking of multi cloud environments. This paper focuses on literature work associated with different variants of RSA in fusion with other methods and a proposed methodology which integrates dual techniques Improved RSA (based on principle of Hamming weight) and SSS (Secret Sharing Scheme) methods to improvise the security of data in cloud environments. The proposed method was compared with existing method taking in one parameter and was been proved that it excels the performance drastically.**

***Keywords*: Hamming weight, Improved RSA, Multi Clouds, Security in Cloud, Shamir Secret Sharing.**

I. INTRODUCTION

Cloud computing, a conspicuous technology, in this digital era, provides the users multitudinous advantages like flexibility to resource utilization, availability, easily manageable and collaborative, sustainability, quality control and so on, thus providing a competitive and strategic edge over other paradigms. It indicates the credible direction at which the technological industry is moving. Each technology has both sides, positive and negative and nothing is fool proof and so cloud computing is no exclusion. Security breach is something that even the leading organizations which are broadly accepted across the world have suffered from and it is dormant hazard in the cloud as well. Though exceptional security measures are deployed, still stocking the confidential data in the cloud can be a precarious task. In spite of pervasive research on cloud, security is still a blockade especially when single cloud is used and thus, there was an upheaval to multi cloud ambiance in the current decade. Henceforth, intensifying the security is imperatively needed. To enhance the security in the multi cloud environments, a hybrid method was been proposed which is a fusion of hamming weight-based RSA and Multi party computations. Organization of the paper is as follows:

Section 2 discusses about Literature Review of RSA Cryptosystem, Section 3 briefs multi-party Computation using multi clouds and emphasizes on proposed methodology, Section 4 deals with comparative analysis of existing and proposed methods and Result analysis and Section 5 focuses on Conclusion and Future work.

II. LITERATURE REVIEW OF RSA CRYPTOSYSTEM

To conquer the security challenges of the cloud era, new security mechanisms are invented very frequently, which acquire in cryptography, as a major element enabling secure articulation over cloud environments. Cryptography is not anew and since ancient days it is used for secure dissemination of data and resources. The first proven usage of cryptography dates back to 1900 B.C [1]. It is application of mathematical techniques and tools to information security aspects such as confidentiality (prevents the disclosure of private information to unauthorized users), integrity (ensures data received is not being altered) and availability (readily available to authorized users) unitedly known as CIA triad.

A. *RSA Cryptosystem and its real time deployment*

Public key cryptography (PKC) also known as Asymmetric key cryptography is based on the concept of dual keys. It is largely used for authentication, key exchange and non-repudiation. Since its origin, many a number of algorithms are been devised where in RSA algorithm is the earlier known across the user community, which was named after its inventors R. Rivest, A. Shamir and L. Adleman and was publicly revealed in 1977 and is used extensively in secure data transmission. RSA algorithm takes an edge over other cryptographic algorithms because of its underlying mathematical structure and perhaps this is the rationality for its acceptance worldwide. A vast applicability of RSA was been found over internet, providing confidentiality and authentication to e-mail. It has become fortitude to provide security to much familiar e-commerce specifically for authentication purpose. Googles GSuite, which has been rated as excellent on PGMags review in February 2017 [2] is based on cloud services and it uses RSA. Also, in many organizations RSA is largely used for employee verification. In today's era, chip based smart cards which are embedded with cryptographic algorithms are used to ensure security, where in some of these cards use RSA in combination with

Revised Manuscript Received on August 05, 2019

Parsi Kalpana , Assistant Professor at Sr Francis College for Women, Hyderabad.India.

other algorithms [3]. RSA SecurID, a two-factor authentication technology used in high-security environments to protect network resources also uses RSA [4].

B. *Strengths and Weaknesses of RSA*

RSA algorithm's efficacy mainly comes from the fact that it is very challenging to computationally factor large integers into primes. Multiplying any two primes is quite easy but achieving the reverse is indeed hard because of factoring. For instance, the RSA Factoring Challenge enacted by RSA Laboratories in 1991, has many moduli still pending to be factored [5]. The Federal Information Processing Standards Publication (FIPS PUB) 186-4 specifies three choices for the length of the modulus, n, to be 1024, 2048 and 3072 bits [6]. The potency of RSA lies in its key size and a unique pair of public and private keys are provided for each user, thus allowing them to interchange the data in a shielded way without a need to exchange secret key beforehand which generally is needed in symmetric methods.

Due to this critical nature of unique key pair, keys in asymmetric methods are technically more costly than their counter parts. A major hindrance to RSA is that the enabling company is not ready to accept that a problem does exist in the key length and it is not willing for upgradation to comply with the computing power of the present and probably the future devices. Thus, RSA algorithms need to revise key generation techniques and enunciate on more stronger keys which cannot be cracked easily and emphasis should be on doing all this within the computation power limits. Although RSA is universally accepted and used cryptographic algorithm, still it has certain limitations which need to be contemplated for it to sustain, to be the master.

C. *Enhancements proposed to improve security of data using variants of RSA in cloud environments*

Rohini et al [7] have proposed a hybrid approach where RSA algorithm together with HMAC was used to enhance the security of data in the cloud. Emphasis was on providing security at various levels like owner level, administrative level and user level. In the proposed framework authors have proved that encryption time using RSA and HMAC is efficient when compared to RSA and Pailier cryptosystem.

Dr. D.I. George Amalarethinam et al [8] proposed ERSA algorithm in which varying key sizes are used to make the encryption process strong so that it will be difficult for the attackers to intrude the data. At the same time, encryption and decryption times are increased proportionally with increase in key size. The proposed algorithm reduces the time of encryption and decryption processes by dividing the file into blocks and enhances the strength of the algorithm by increasing the key size.

Srinivasan Nagaraj et al [9] proposed that the randomness of the key generated increased the security of the data and also the encryption process consumed significant amount of resources. They suggested that this can be enhanced by encrypting multimedia data which needs secured transmissions over unsecure channels.

Vishwanath S Mahalle et al [10] suggested a hybrid approach which uses RSA and AES algorithms, a combination of Symmetric and Asymmetric algorithms, to provide data security to the user in cloud. In this approach three keys are used. Public key for encryption and private and secret keys for decryption processes. Authors mentioned that the main advantage of the proposed method is keys are generated based on system time and so no intruder can guess them.

R. Thilagavathy et al [11] proposed a modified RSA encryption algorithm with longest common sub sequence of a string (LCS) and the implementation of the proposed model was run in Net Beans IDE environment. The encrypted and decrypted files are compared and the correctness of proposed system is proved.

Khalid et al [12] proposed FAST cloud-RSA which is based on generalized Multipower RSA in order to speed up the efficiency of RSA. FAST cloud-RSA was been implemented and compared with cloud-RSA and it was proven that proposed method out performs the decryption time to a greater extent compared to cloud-RSA.

III. MULTI PARTY COMPUTATION USING MULTI CLOUDS

The State of art research is going on usage of multi clouds. Multi-party computation is a sub field of cryptography where in multiple users can compute a function and yield a result of common interest without revealing their own data or inputs. Since inception of multi-party computation, many protocols came into existence among which Shamir secret sharing is prominent. It is a form of secret sharing, where a secret is splitted into parts, giving each participant its unique part, where some or all parts are needed in order to reconstruct the secret.

Using multiple cloud ambiance and performing a multi-party computation can be constructive for safe guarding the secrecy of user's vital data. Recent research into multi clouds combined with multi-party computations was been surveyed in my previous paper [13]. Using multiparty computation, the user can enumerate shares of his/her data using a secret sharing scheme such as Shamir's and disburse those shares to different clouds. The clouds will jointly compute the function of interest on these shares, acquainting themselves with each other when and where needed, thus ensuring the security of the data, until and unless the cloud providers collude to open shares with each other. Compared to the other schemes, Shamir's secret sharing scheme is impeccable mechanism as the secret cannot be rebuilt using less than the required threshold. The more the number of shares, the harder it is to find the threshold value.

As discussed, RSA being the most widely used PKC algorithm requires considerable amount of study and enrichment to get the best possible expertise in terms of execution time and memory utilization.

A. *Proposed Methodology*

To improve the security aspect of RSA, it was been improvised by using principle of Hamming weight. Hamming weight is the number of symbols that are different from the zero symbol and is used in several disciplines including coding, information theory and cryptography to name a few. IHRSA (Improved Hamming weight-based RSA) was been proposed and it was been integrated with the concept of Secret Sharing methods to enhance security of data on the

cloud. IHRSA security module is a public key encryption, which is used to encrypt and decrypt the data in the cloud environment. The IHRSA digital encryption efficiency is based on the strong prime number used for key generation. The strong prime number is used to create the public and private key then it is used with Hamming weight and Euler's method to reduce the computational time. IHRSA method is based on the difficulty of the factorization of two large prime numbers and is measured as factoring problem. In the proposed method, the user first establishes a connection with server (Cloud) and during this, key generation takes place where server uses Shamir's Secret Sharing (SSS) scheme to generate random shares from a secret key and sends them to the user. Also, encryption and decryption keys of RSA are also generated based on the concept of hamming weight internally. User encrypts the confidential data using proposed IHRSA (Improved Hamming weight-based RSA). Encrypted data will be stored on a local server (or cloud) and the random shares are generated from SSS secret key and these shares are stored on multi clouds uniquely. Decryption process involves usage of shares which were generated during key generation followed by IHRSA, thus avoiding unauthorized access to data, thereby ensuring the security of data. The proposed method does not allow decryption to occur until the shares are retrieved correctly as per required threshold value. If and only if, minimum number of shares required are obtained, the process allows them to use decryption key and get back the original data further. Thus, the proposed method is specified in four phases namely key generation phase, encryption phase, share retrieval phase and decryption phase. For all phases to occur fortuitously, user authentication is necessary before key generation phase and also before decryption phase. User authentication is performed by using required credentials like secure login id and password. If authentication is successful, the user can generate key and encrypt the data efficiently and similarly for decryption to occur, first share locations must be specified followed by retrieval, if it is successful, then again user authentication is performed, which allows decryption phase. If an intruder obtains decryption key also, the original data cannot be obtained since the proposed method does not allow it to happen, because for an intruder to get the data, first shares must be retrieved which are preserved on different clouds, which is not possible since these shares are randomly generated and stored, thus providing the security to the vital data. For any user to obtain the data, primarily location of clouds where the shares are safeguarded must be known first, then followed by retrieving them which then finally allows to decryption phase to occur, thus decryption is not straight forward approach here, henceforth security is improved in the proposed method. The following block diagram "Fig.1" depicts the proposed methodology. Most of the encryption methods consist of the large module, which increases the power consumption and computational time. This method helps to optimize both encryption and decryption times, thus increases the speed of the process and elevate the system.

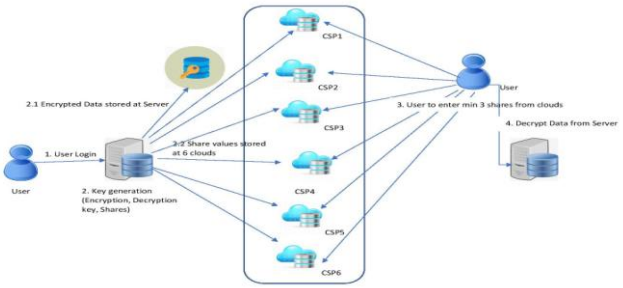

Fig. 1. Block diagram of proposed method

B. *Results*

The proposed methodology is a hybrid approach which integrates hamming weight-based RSA and Shamir secret sharing scheme of multi-party computation protocol. Evaluation of the proposed method was been bifurcated into 4 phases namely key generation, encryption, shares retrieval and decryption and then total time was been computed and the method was been deployed on .NET Framework with Windows 64-bit Operating system and coding was done in C#. The pilot version was been evaluated successfully. For better results, evaluation was been iterated around 10 times with a key size of 128 bit and a sample employee dataset of size 32Kb was been considered and obtained less encryption and decryption times. "Table I" depicts the values obtained during the evaluation process.

Table I. Evaluation times of different phases of proposed method

No of Iterations	Key Generation Time(ms)	Encryption Time(ms)	Shares retrieval time(ms)	Decryption Time(ms)	Total time(ms)
1	92	290	26	2431	2839
2	159	371	29	2428	2987
3	165	355	26	2484	3030
4	154	474	26	2445	3099
5	198	417	35	2445	3095
6	125	356	32	2401	2914
7	158	374	27	2404	2963
8	143	393	26	2476	3038
9	129	423	34	2479	3065
10	161	349	27	2436	2973
Average	**148.4**	**380.2**	**28.8**	**2442.9**	**3000.3**

In this scenario of iterations, key generation time is more than share retrieval time as key generation involves generation of encryption key, decryption key followed by secret key from which shares are generated. Share retrieval is less, because all the values are related to successful evaluation. For unsuccessful scenario, share retrieval time increases depending on improper location specifications or improper no of shares. The following figure "Fig 2" depicts the graph related to the above obtained values.

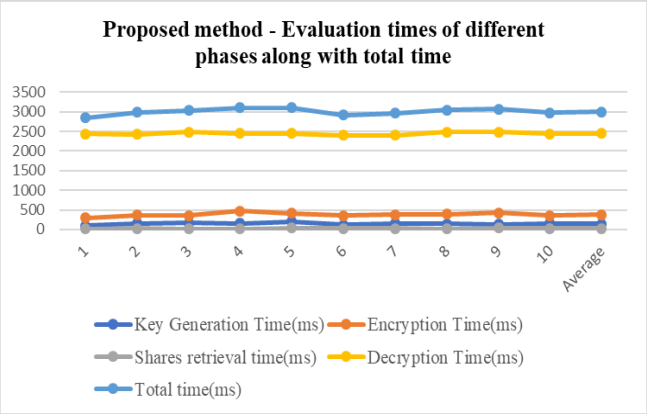

Fig. 2. Graph related to data pertaining to Table I.

IV. COMPARATIVE ANALYSIS OF EXISTING AND PROPOSED METHODS

In [8], authors have proposed ERSA algorithm where varying key sizes were used to make strong encryption phase. Their method based on the dividing the data into blocks and enhancing security. In the proposed method, emphasis was not data splitting rather it was an integrated approach where shares generated by a secret sharing method are divided and stored at different clouds. For comparative analysis, data size of 32kb was been considered as authors did in [9], but comparative analysis was done only for 128-bit key size and obtained better results. Even though the proposed method consists of 4 phases contributed for evaluation, the overall performance obtained was improved than the results obtained by authors in [8] for key size of 128 bits and data size of 32 kb. The following table "Table II" interprets the comparison of both methods:

Table II. Comparison of existing and proposed methods

	Encryption Time(ms)	Decryption Time(ms)	Total Time(ms)
ERSA (Existing)	1489	1873	**3362**
IHRSA&SSS (Proposed)	380.2	2442.9	**3000.3**
	Key generation, retrieval	**177.2**	

As we are in fast track digital era, performance of the system and run time analysis plays a prominent role. For the user who want to store the data securely, encryption should be done at a higher speed along with maintaining the confidentiality, integrity and authenticity. Figure "Fig 3" shows the average encryption time obtained after 10 successful evaluations and it's clear that there is a drastic difference in the encryption times of the both where the encryption time of proposed method is approximately 1/4th of existing method's encryption time. Thus, there is a greater enhancement in terms of encryption.

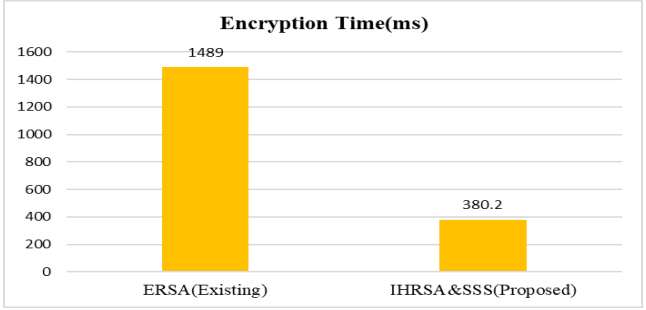

Fig. 3. Encryption times of ERSA and IHRSA&SSS

Below figure, "Fig 4" shows that the decryption time obtained in the proposed method has been increased compared to existing since decryption is not straight forward mechanism here. For successful execution of decryption phase to happen, first location of shares must be specified followed by required number of shares retrieval. Only if shares are retrieved accurately, then decryption phase is activated hence increasing decryption time. But time variation is less and it can be stated as reasonable because focusing on security of data is the need of the hour and it comes with an additional increase in time.

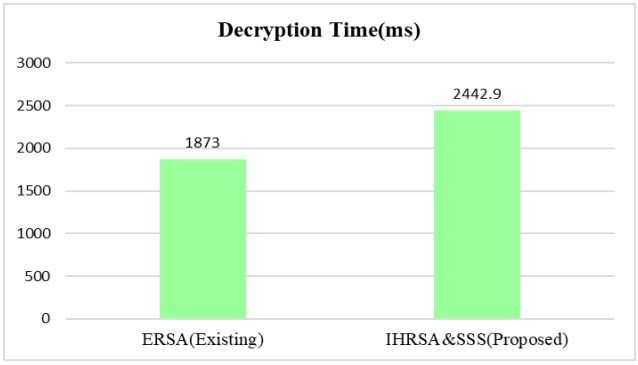

Fig. 4. Decryption times of ERSA and IHRSA&SSS

The below figure "Fig 5" shows the encryption and decryption times obtained by both methods and also the time for key generation and shares retrieval of proposed method. The overall evaluation time after summing up key generation, encryption, shares retrieval and decryption of proposed method is less compared to the total time obtained in existing method, thus even though the number of phases increased to accomplish more security, the proposed method outperforms the overall execution time of existing method.

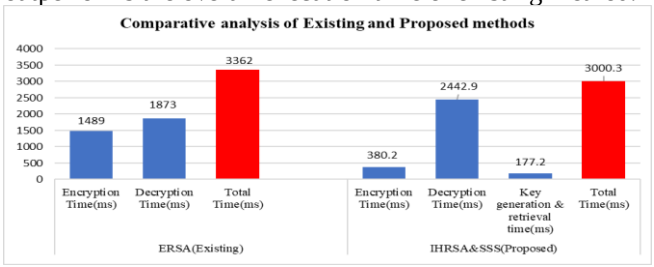

Fig. 5. Graph depicting encryption and decryption times of ERSA and HRSA&SSS methods

V. CONCLUSION AND FUTURE WORK

The proposed method optimizes the system and leverages the execution time. As Secret sharing

approach was been used along with IHRSA, decrypting the data by colluder is impossible thus strengthening the security of data. Multi cloud approach for complementing security and privacy of data is a leading evolution in this computer epoch where cloud is the utmost used distributed system based on internet. The data sharing method are computationally modest in comparison with the traditional encryption techniques. Thus, when the data is encrypted using data sharing scheme it is affirmed to be more concealed and adamantine to compromise. More research and study in terms of employing strong encryption mechanisms and combining them with partitioning data or application among multiple clouds brings out a promising future for multi cloud architecture and can be used widely for any domain. Future work is to deploy the proposed methodology of IHRSA and Secret Sharing on multi clouds on different data sets and key sizes ad to come up with an ideal solution which can deal with present security scenarios.

REFERENCES

1. G. C. Kessler, An Overview of Cryptography, Boca Raton: Auerbach Publications (2017).
2. B. Darrow, PointCloud: Fortune.com, 1 Feb 2017, http://fortune.com/2017/01/31/google-g-suite
3. Shireen Nisha, Mohammed Farik, RSA Public Key Cryptography Algorithm–A Review, International Journal of Scientific & Technology Research, Vol 6, Issue 07, July 2017, ISSN 2277-8616.
4. V. Beal, Term: Webopedia.com, QuinStreet Enterprise, http://www.webopedia.com/ TERM/R/rsa_secure_id.html
5. Wikipedia, 299 March 2017, https://en.wikipedia.org/wiki/RSA_numbers
6. Information Technology Laboratory, Digital Signature Standard (DSS), National Institute of Standards and Technology, Gaithersburg, 2013.
7. Rohini, Er Tejinder Sharma, Proposed hybrid RSA algorithm for cloud Computing, Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), IEEE Xplore Compliant - Part Number: CFP18J06-ART, ISBN:978-1-5386-0807-4.
8. Dr. D.I. George Amalarethinam, H. M. Leena, Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud, World Congress on Computing and Communication Technologies, 978-1-5090-5573-9/16 $31.00 © 2016 IEEE DOI 10.1109/WCCCT.2016.50
9. Srinivasan Nagaraj, Dr.G.S.V.P.Raju, V.Srinadth, Data Encryption and Authentication Using Public Key Approach, Elsevier Procedia Computer Science 48, pp. 126 – 132, 2015.
10. Vishwanath S. Mahalle, Aniket K. Shahade, Enhancing the data security in Cloud by implementing Hybrid (Rsa & Aes) Encryption Algorithm, IEEE, doi: 10.1109/INPAC.2014.6981152, pp. 146-149, 2016.
11. R. Thilagavathy and A. Murugan, Secure the Cloud Data Transmission using an Improved RSA Algorithm, Indian Journal of Science and Technology, Vol 10(12), ISSN (Online): 0974-5645, DOI: 10.17485/ijst/2017/v10i12/103770, March 2017.
12. Khalid El Makkaoui, Abderrahim Beni-Hssane, Abdellah Ezzati, Anas El-Ansari, Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing, The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017), ScienceDirect, Procedia Computer Science 113.
13. Parsi Kalpana, Perlustration on Recent Research into Multi Clouds integrated with Multi Party Computation, Accepted for publication in International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249-8958, Volume 8, Issue 6, August 2019.

AUTHORS PROFILE

Parsi Kalpana is currently working as Assistant Professor at Sr Francis College for Women, Hyderabad. She is pursuing PhD in Computer Science Engineering from Osmania University and holds 2 Masters Degrees, M. Tech in Computer Science & Engineering from JNTUH and Master of Computer Applications from OU. She possesses more than 16 years of teaching experience and has published 11 papers in various International Journals and Conferences. Her area of interest is Cloud Computing and its security mechanisms.