International Journal of Computational Intelligence Systems
Vol. **13(1)**, 2020, *pp.* 36–43
DOI: https://doi.org/10.2991/ijcis.d.200110.001; ISSN: 1875-6891; eISSN: 1875-6883
https://www.atlantis-press.com/journals/ijcis/

Light Weight Proactive Padding Based Crypto Security System in Distributed Cloud Environment

N. Indira[1,*], S. Rukmanidevi[2], A.V. Kalpana[3]

[1]*Research Scholar, Anna University, Dept. of CSE, Panimalar Engg. College, Chennai*
[2]*Professor, Department of CSE, R.M.D. Engineering College, Thiruvallur, Tamil Nadu, India*
[3]*Asst. Professor, Dept. of CSE, R.M.K. Engg. College, Chennai*

ARTICLE INFO

Article History
Received 08 Oct 2019
Accepted 20 Dec 2019

Keywords
Cloud security
Cryptanalysis
Key policy
Privacy
Prime padding

ABSTRACT

The organization maintains various information in cloud which is a loosely coupled environment. However, the nature of cloud encourages the threats in different level. Among them the data security has been a keen issue being identified and challenges the service provider. To improve the data security performance, different algorithms have been discussed, but suffer to achieve higher performance in data security. To design more secured data security algorithm, a light weight proactive padding based crypto security system (LPP-CS) is presented in this paper. The method generates keys to support the crypto systems based on the prime values. The keys are generated from the set of prime numbers which have been used to pad the cipher text generated. The end user will be given with the key which is generated and distributed at the assignment. The encryption is performed in block level and for each block of data different keys has been used which challenges the adversary highly. The selection of prime factors and keys are suitable for any specific time window and has been iterated frequently. The proposed LPP-CS algorithm improves the performance of cloud data security with less time complexity.

1. INTRODUCTION

Cryptography is the process used to help to increase data security. Cryptography nearby security of data from theft or change could in likewise be utilized now for confirmation of clients. As of late, cryptographic strategies are fundamentally of two sorts to be specific: public and private key cryptography. Symmetric key cryptography is the procedure in which the same keys are utilized for encryption and the decryption stage. Open key cryptography is utilized fair when one key is utilized for encryption and a substitute key is utilized for the decrypting. The most prominent favored point of view of symmetric key cryptography over the public key cryptography is that it is significantly simpler to deal with the key, since fair a single key is utilized for both the procedure of encrypt and decrypt.

The key, be that as it may, ought not to be uncovered to the outside world.

In spite of the fact that cloud has numerous preferences, it has a few drawbacks as well, and one of them is security issue. Cloud computing has a number of security issues such as data access control, identity management, risk management, auditing and logging, integrity control, infrastructure and dependent risks as flow depicted in Figure 1. If any organization is using cloud computing, they should provide their important data to service provider. The possibility of sensitive information going to wrong hand is increasing due to

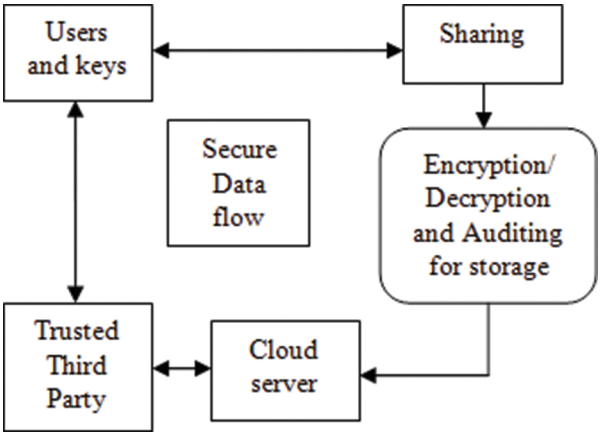

Figure 1 | Cloud security dataflow.

cloud services being easily accessible and available for all. The organizations cannot take risks with their sensitive information. Hence, there is a need to resolve the security issue of cloud computing. Figure 2 is depicting data storage security in cloud.

Further, the security concerns regarding information sharing and attacks have been highlighted. To overcome from these assaults security measures with respect to information security and authentication are examined in detail coming about in utilization of cryptography as a solution. The comparative examination of different light weight encryption and authentication calculations are carried out. This analysis comes about appear that the light weight

[*] *Corresponding author. Email: indiranatarajan13@gmail.com*

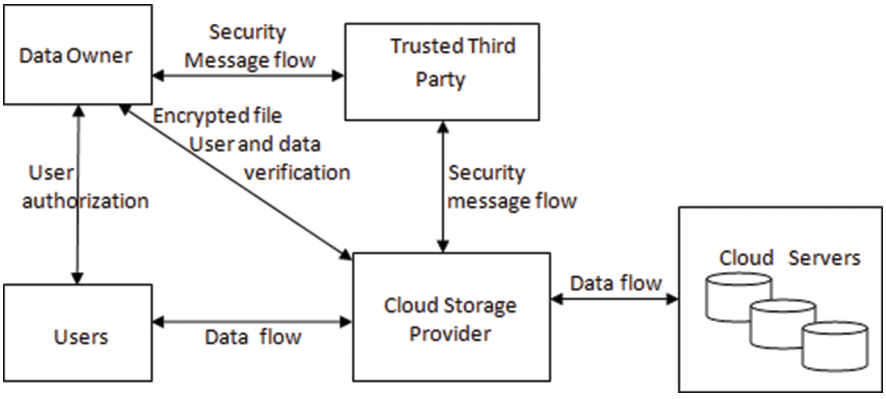

Figure 2 | Data storage security in cloud.

algorithms have great performance as compared to customary cryptography algorithms in terms of memory prerequisite, their operations and power consumption. Moreover, a few investigate directions characterized in which advance work can be done on light weight cryptography algorithms.

Providing secure data to the users includes providing security during data transfer and the data storage. The existing scheme for imparting security to data is concerned with data storage security and does not take into account of the intruding possibilities that could take place during data transfer. Moreover within the existing framework, the third party evaluator is given get to view the client information which postures an expanded risk to the client information as the intruder himself may mask as the third party. As the security is provided only for data storage, occurrences of data loss during transfer and intruders penetrating into the network increases. A novel cloud data security model is proposed to overcome the different in-efficiencies in the current scheme of cloud security. In the proposed methodology, in addition to data security, it concentrates on providing security to transfer data using encryption technique and the approach makes the data un-available to the third party.

For each block level of data, the proposed strategy selects a separate encryption key to infix the cipher text as improved security. Initially prime padding factors are generated and then state formulation matrix is padded with substitution keys. This makes row shifting; interchanging of column for the shift data is performed. Prime padding decryption is performed by removing the padding from the blocks with respect to padded data count. The remainder of the paper is organized as follows: In Section 2, related works on secure storage are discussed. In Section 3, proposed framework Light weight Proactive Prime padding based crypto security architecture and proposed prime factor key generation, prime padding encryption and decryption algorithms are discussed. The results and security of light weight proactive prime padding based crypto-file security (LPP-CS) system in terms of execution efficiency, security, time complexity and frequent occurrence are analyzed in Section 4 followed by the conclusion in Section 5.

2. LITERATURE SURVEY

Security of information is getting to be an imperative challenge for a wide range of applications, including communication frameworks [1,2] (with high security prerequisites), secure storage supports, digital video recorders, smart cards, cellular phones. Resistance against assaults that is known is one of the most properties that an encryption calculation has to give.

The fundamental issues to be tended to by a network security capability are investigated by giving a tutorial exercise and study of cryptography and arrange security innovation [3]. In the case of simple cryptosystems based on factoring large integers however, an inevitable tradeoff seems to exist between one-wayness and chosen cipher text security [4]. This incompatibility, which was observed for factoring-based signature schemes as well. Allow users to audit the cloud storage with very light weight communication and computation cost. The reviewing result not as it were guarantees solid cloud capacity rightness guarantee [5], but too at the same time accomplishes quick information blunder localization, i.e., the Recognizable proof of getting into mischief server. For the previous concern, information was encrypted and sometime recently outsourcing is the only way to secure information privacy and combat spontaneous get to within the cloud and past [6]. But encryption too makes sending conventional information utilization administrations. Emphasize that in spite of the fact that there are numerous technological approaches that can move forward cloud security, there are as of now no one-size-fits-all arrangements [7] and future work has to tackle challenges such as service level agreements for security, as well as holistic mechanisms for ensuring accountability in the cloud.

On ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations [8]. The troubles and potential security issues of direct extensions with completely powerful information updates are recognized from earlier works and also present day encryption methods [9] and afterward it is told that the best way to develop a rich verification scheme for the consistent coordination of these two notable highlights in the convention structure. Security challenges in public issues relating to the cloud data storage methods and security in virtual environment [6,10,11]. To solve privacy preserving public auditing scheme for providing data storage and security in cloud using public key Rivest-Shamir-Adleman (RSA). A hybrid crypto [12] idea is proposed, which is the mix of new symmetric [13] and message processing capacity for security function in RSA Security standard. Play fair cipher is a fascinating information encryption strategy with a medium level of complexity and along these lines, is appropriate for security of wireless and portable systems [14]. Different sizes of the matrices used

for the keys were studied, RSA and Advanced Encryption Standard (AES) [16,17] for verifiable resources. But no study has been done as such far that gives a near examination of various network sizes of a key. Cloud system is an emerging technology in which security is the most challenging issue [18,21]. RSA encryption calculation is an old encryption calculation which fails in keeping up security level of information in transit if the estimation of public key is accomplished by the attacker.

3. LIGHT WEIGHT PROACTIVE PADDING BASED CRYPTO SECURITY SYSTEM

The objective of the proposed work is to design and develop a technique that mediates the user and the operations to achieve security using light weight proactive key padding. As realized that encryption gives strong security to data very still. At first proposed technique is appropriate for limited quantity of data. The performance and security issues have considered in the proposed work since it definitely realized that in certifiable situations, these are mind boggling issues and experts should be used who understand all available options and the impact for each particular customer environment. This work will demonstrate less query execution time from proposed procedure. The focusing encryption and decryption for secured data be the encrypted information which should be in unreadable, to extend user authentication.

- Proposed concept providing security whenever transmitting information from request authenticated to another person with addition prime padding because it's important to protect the information while it is in transit. Proposed technique is another cryptography algorithm for encryption and decryption at client end on client data.
- The proposed algorithm depends on a symmetric block cipher. The performance and quality of proposed method is required to be superior to traditional cryptographic calculation and exceptionally successful against brute force attack.

Cryptographic file frameworks scramble and additionally secure the integrity of the put away information utilizing encryption and information validation dependent on request response as appeared in Figure 3. The LPP-CS is used because the underlying storage provider is not trusted to prevent unauthorized access to the data with verifiable third party auditor (TPA) auditing. Therefore proper access control cannot be enforced light weight security, to enhance the public key crypto a system to the data doesn't break using key that are being replaced. In a system using encryption, access to the keys gives access to the data. Therefore, it is important that the security provider manages the encryption keys for the file system. Presenting a different key administration, which must be synchronized with the security supplier giving access control data, just convolutes matters. Analogously, the security provider should be responsible for managing integrity reference values using public key standards, such as hashes of all files. File systems with enhanced capabilities such as cryptographic protection exist in two forms: either as a monolithic solution, realized within an existing physical record framework that uses a basic block storage supplier as stackable or layered virtual document framework, which is mounted over another (physical) document framework. Proactive security begins to generate prime padding factors for public key cryptography. Generating state formulation modulo matrix for padding the keys to data substitution makes shifting rows and encrypts data. Mix the columns state interchanging of shift data auditing is introduced in cloud computing to deal with secure data storage. Evaluation is a procedure of verifying the clients information completed either by the customer or by a TPA. Auditing helps to maintain the integrity of client's data stored in the cloud. The auditing procedure can be classified into two kinds: Initial one is private auditing where customer or information proprietor is permitted to check the integrity of the information which is stored. But it increases verification overhead of the client. Second is public examining, which permits anybody, to challenge the cloud server and performs information confirmation check with the assistance of TPA. TPA is the outsider reviewer who will review the information of information proprietor or customer. The TPA has skill and abilities that users don't. TPA ought to effectively audit the cloud data storage without requesting for the local copy of information state.

3.1. Light Weight Encryption

Encryption procedure changes over the first information into cipher data with the assistance of prime factor. Prime factor calculation is a two standard key cryptography technique, which uses secret key to encrypt the original information and send this key with encoded data to the recipient. The hazard associated with symmetric cryptography is the moving of secret key over the web. AES block cipher substitution algorithm is used padding key cryptography method. The risk of symmetric cryptography is overwhelmed by having secure strategy for imparting a symmetric key to different clients, safely sharing the key by encryption of the key, sender and recipient to concede on the secret key already and by making an adequately longer key.

A. Key padding

The Padding symmetric cryptography uses prolactin additional padding enhances the asymmetric cryptography uses a pair of keys to encrypt and decrypt message. One of these two keys is known as public key as it is distributed to others and the other is called private key which is kept secret normal than generating group keys. Ordinarily public key padding is utilized to encrypt any message which must be decrypted by the relating private key. There are fundamental properties that must be fulfilled by the asymmetric cryptography.

- The key generation procedure ought to be computationally proficient.
- Sender should be able to compute the cipher text by using the public key of the receiver for any message. The beneficiary ought to have the option to decrypt the plain text effectively by utilizing his own private key.
- It is unthinkable or if nothing else unfeasible to process the private key from the comparing public key. It is computationally infeasible to calculate the plain text from public key and cipher content.

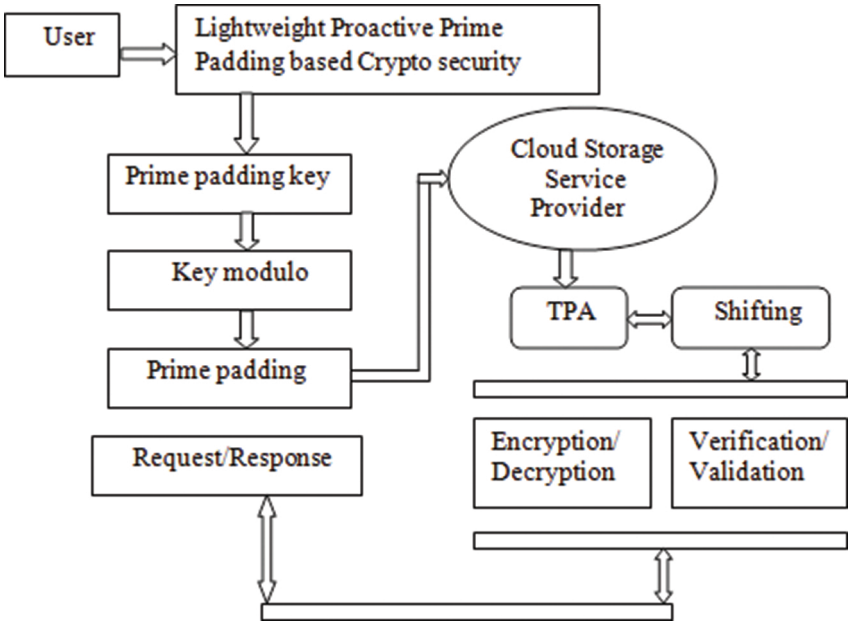

Figure 3 | Architecture diagram for proposed system.

B. AES circular shifting

As an, AES shares a secret key to encrypt with proactive security and decrypt any message and works on block substitution. Padding key with the data enhances the transition rotation and maintains the blocks as key lengths and the resulting maintains the shifting index which is favor for security enhancement respectively to indicate the length in bits of the key.

C. TPA auditor

As the users do not have time to check their uploaded data periodically it delegates this task of auditing to TPA. Reviewer has essential ability to check the accuracy of information stored in the capacity server. Auditor compares the hash key of file, audits the file and sends audit status to client. Auditor assesses and uncovered the danger of cloud storage benefits for clients upon requesting.

D. Integrity checking phase

In this stage customer checks occasionally for integrity of his/her information stored in the cloud. For this, customer depends on evaluator for inspecting the data. When client requests auditor for auditing, the cloud server gives hash value of data to auditor. Auditor will compare hash values of file and audits the data integrity of file. After auditing, auditor sends the audit status of file to client.

3.2. Prime Factor Key Generation

This stage is used for generating two keys, namely, Public Key E and Private Key D. Generally Proactive prime Padding algorithm uses two prime numbers. In addition to that, two progressively prime numbers, in particular, PR1 and PR2 are incorporated into the proposed algorithm LPP-CS. The next step of the algorithm computes two values such as M and N. Four prime numbers are multiplied and computed as M. For N computation, it uses two prime numbers. This is done to increase the complexity of the encryption portion.

Algorithm 1: Key generation of proactive padding algorithm

Input: Key Set Ks
Output: Public Key Pk, Private Key Prk
Start
Read key set Ks.
Select two random prime numbers P and Q.

$$P \rightarrow \int_{i=1}^{100} \text{Random}\left(\sum \text{PrimeNumbers}\,(1,100)\right)$$

$$Q \rightarrow \int_{i=1}^{100} \text{Random}\left(\sum \text{PrimeNumbers}\,(1,100)\right)$$

Compute Public Key Pk.
Compute $N = \frac{(P \times Q)}{100}$

$$Pk = \int_{i=1}^{size(Ks)} Ks\,(N)$$

Compute Private Key Prk.
Compute $M = \frac{P/Q}{100}$

$$Prk = \int_{i=1}^{size(Ks)} Ks\,(M)$$

Stop

The proactive prime padding algorithm generates public and private keys to support encryption and decryption in data transmission.

3.3. Prime Padding Encryption

Encryption procedure changes over the original information into cipher data with the LPP-CS calculation. Algorithm is prime padding cryptography strategy, which uses secret key to encrypt

the plain text and send this key with encrypted information to the recipient. The message must be a number less than the smaller of P and Q. However, at this point we don't know P or Q, so in practice a lower bound on P and Q must be published. This can be somewhat below their true value and so isn't a major security concern.

Algorithm 2: Encryption algorithm

Input: Plain Text Pt, Key Set Ks, Public Key Pk, Private Key Prk
Output: Cipher Text CT
Start

Read Pt, Ks, Pk, Prk

$$\text{Generate Number of blocks Nb} = \int \text{Random}(1, 20)$$

$$\text{Split plain text Tb} = \int_{i=1}^{Nb} \text{Split}(\text{Pt}, \text{i})$$

For each block B

$$\text{Padding bits Pb} = \int \text{Random}(1, 20)$$

$$\text{Cipher Text Block CTb} = \int \text{Encrypt}(\text{Tb}(\text{B}), \text{Prk})$$

$$\text{Cipher Text Block CTb} = \int \text{Padding}(\text{CTb}, \text{Pb}(1, 0))$$

End

$$\text{CT} = \int_{i=1}^{Nb} \sum \text{CTb}(\text{i}) \cup \text{CT} \cup Nb$$

Stop

The prime padding encryption process enhance with the initial round padding prime factors which is enhancing the possibilities of exponent factors. E-Modulo performs only the supportive transitions key transformation on the state array and provides the security, as this is the only stage that makes use of the secret key.

3.4. Prime Padding Decryption

A decryption focuses on the issue of key ensuring the responsibility of data accumulating in security check. Decryption involves reversing all the steps taken in encryption using inverse functions. Specifically, consider the assignment of permitting an outsider inspector (TPA), for the verifiable key examining to permit to authenticate for checking the dependability of the dynamic data set away in the cloud check. The introduction of TPA kills the relationship of the client through the assessing of whether his data stored in the cloud is without a doubt in generally security concerns not permitted.

Algorithm 3: Prime padding decryption

Input: Private Key Prk, Public Key Pk, Cipher Text Ct
Output: Original Text OT
Start

Read Prk, Pk, CT

$$\text{Number of blocks Nb} = \int \text{ExtractLost}(2, \text{CT})$$

Split CT into Nb number of blocks

$$\text{Block set Bs} = \int \text{Split}(\text{CT}, \text{Nb})$$

For each block

$$\text{Remove padding b} = \int_{i=1}^{Nb} \text{Remove}(\text{Bs}(\text{i}), \text{Nb})$$

$$\text{Block text bt} = \int \text{Decrypt}(\text{b}, \text{prk})$$

$$\text{OT} = \int \text{OT} \cup \text{Bt}$$

End

Stop

The above discussed algorithm shows how the prime padding decryption is performed on the given cipher text. The method splits the cipher text into number of blocks and for each block the padding is removed according to the number of padded data. The decrypted text has been given to the user. The usage of prime numbers instead of random numbers showed the strength of encryption process. Because it is difficult to identify a prime number rather than a random number, it gives a way to improve the strength of the key. The time spent for encryption and decryption procedures are for the most part lesser than with random numbers.

4. RESULT AND DISCUSSION

The Resultant proves the security of key standard. LPP-CS cryptography encryption be designed to improve the security by means of the fact of accuracy, time complexity to the user roles had the great impact of security access to cloud environment. The resultant proves the privacy of security standard which has been tested with client server role request response verifiable access control. Test case generated by configuring the Microsoft intent framework tool designed to process with SQL server data base has right user access permission which to access with private and public users.

Table 1 holds the parameters that are used to calculate security concerns implemented by LPP-CS crypto policy. The users can access with thousands of files with trust authority and proves have high impact of evaluation sectors on privacy concerns.

The graph given below shows that the analysis of various performance tested by comparison of previous methods.

Figure 4 shows clearly reveals that the speed of encryption and decryption of the proposed algorithm LPP-CS outperforms the time of these processes of High Speed and Secure.

Table 2 shows the efficiency of execution state processed between encryption and decryption using LPP-CS standard. LPP-CS provides a substitution mean time 17.3 ms as well as AES cipher policy. This implementation had much improved performance compared to previous methods, such as Data Encryption Standard (DES), Random Round Crypto Security Encryption Standard (R2R-CSES).

Analysis of security performance gathers the information among various users at the time of access between authorized and unauthorized users. Time of access the original user be access the security

Table 1 | Details of processed parameters.

Parameter	Name
Service provider	Cloud service provider
Data processed	File type, Clair text
File size	25 MB, 50 MB, 75 MB nearer
Number of users	1000

concerns to access the key. The attacks from an unauthorized, try to access the service violated time preference as well as proposed system blocks.

In Figure 5, security performances can be analyzed through total number of vulnerabilities of attacks carried out by un-authenticated process that leads to file decryption by getting plain text.

Analysis of security performance gathers the information among various users, at the time of access between authorized and unauthorized users.

Table 3 shows the comparative analysis of security LPP-CS has 95.2% performance well to dissimilar methods and this implements great performance with more efficiency than previous methods.

Time complexity:

$$\text{Ts} = \frac{\textit{Total number of blocks per bits} \times \textit{Two phase encryption}}{\textit{Time taken}\,(s)}$$

Figure 6 shows the processing time taken executed by different state by different file size, LPP-CS provides a least time 15.2 ms as well as AES cipher policy. This implementation had much improved performance compared to previous methods. Further the time can be improved by chaining. In this, each block of plaintext is applied by Exclusive OR(XOR) operation with the past block of cipher content before encryption. Because of this XOR procedure, a similar block of plaintext will never again bring about indistinguishable cipher content being delivered. Cipher block chaining gives a predictable method to scramble and unscramble huge information. In a block cipher process, content that are stored in blocks are treated as confined units to be encoded and unscrambled successively.

Table 4 shows the comparative analysis of time complexity of LPP-CS produce well performance well to dissimilar methods and this implements great performance with more efficiency than previous methods.

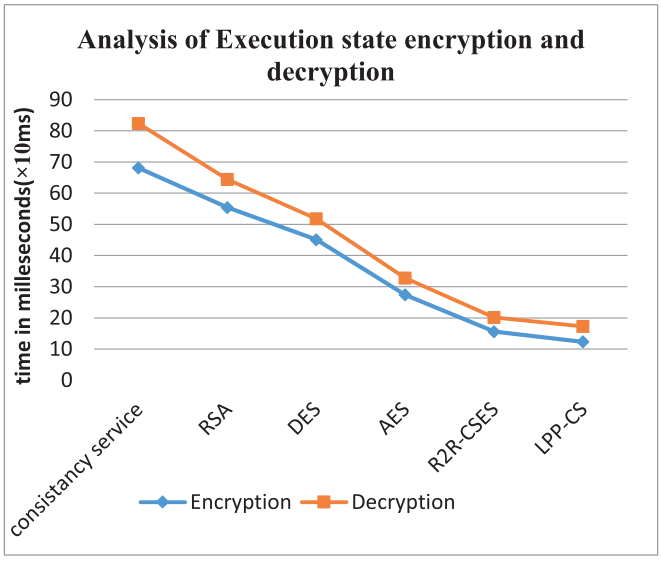

Figure 4 | Comparison of execution efficiency.

Table 2 | Comparison of execution efficiency.

Methods Explored	Execution Time (ms)	
Consistency service	68.1	82.4
RSA	55.4	64.4
DES	45.1	51.8
AES	27.4	32.8
R2R-CSES	15.6	20.1
LPP-CS	12.3	17.3

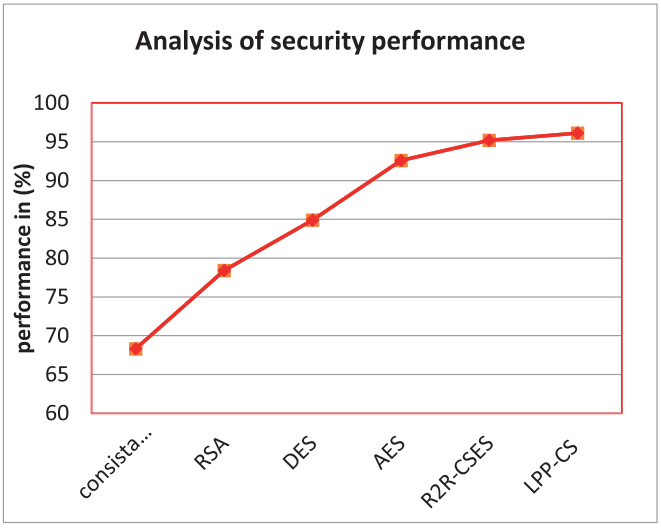

Figure 5 | Comparison of security analysis efficiency.

Table 3 | Comparison of security analysis.

Methods Explored/ Users	Security Analysis (%)					
	Consistency Service	RSA	DES	AES	R2R-CSES	LPP-CS
50 users	68.3	78.3	84.9	92.6	95.2	96.1
100 users	70.3	80.3	86.4	94.3	95.8	96.7
150 users	72.3	83.4	87.2	96.4	96.7	96.9

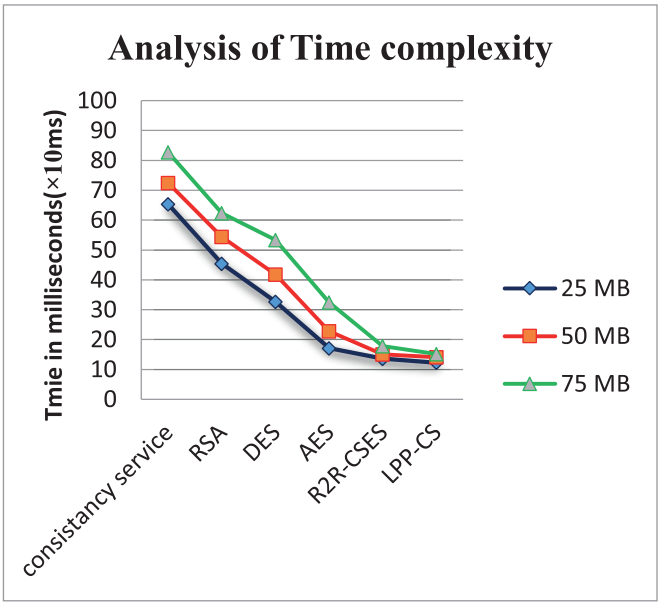

Figure 6 | Comparison of time complexity.

Table 4 Comparison of security analysis.

Methods Explored/ Users	Comparison of Time Complexity					
	Consistency Service	RSA	DES	AES	R2R-CSES	LPP-CS
25 MB	65.3	45.4	32.7	17.1	13.6	12.3
50 MB	72.4	54.4	41.8	22.8	15.1	14.1
75 MB	82.7	62.4	53.3	32.5	17.8	15.2

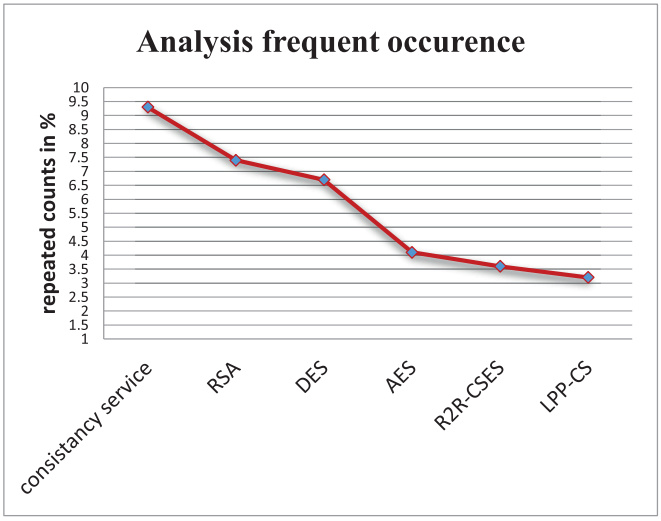

Figure 7 Comparison of frequent occurrence.

Frequent occurrence state

$$(\mathrm{FS}) = \frac{Repeted\ block\ of\ cipher}{Total\ number\ of\ cipher\ blocks\ occurence}$$

Figure 7 shows the frequent occurrence of crypto policy encryption cipher text that is compared by different methods and it shows clearly our implementation method has produced efficient redundant frequency state than previous methods. Frequent occurrence is the investigation of letters or gatherings of letters contained in a cipher message trying to partially uncover the message. Certain letters and collection of letters show up in differing frequencies are taken. By knowing usual frequencies of letters in communication, the sample plain text is created. This plain text is encrypted by various encryption methods and the repeated counts are recorded. By this it is resolved the words that are made sense of and utilizing their letters to break more words, in the long run uncovering the whole message. We can likewise search for cases of repeated letters as just a couple of letters repeat in such a design in common language.

Table 5 shows comparison of frequent occurrence LPP-CS has 3.6% performance well to dissimilar methods and this implements great performance with more efficiency than previous methods.

5. CONCLUSION

In this paper, LPP-CS security encryption standard algorithm has been implemented. This method process the security in two phase round and random key levels according to the encryption. For each level of data, the method selects a separate encryption key to embed the cipher text as improved security. The circular shifts enhance the substitution in prime padding security based on encryption and decryption without use of random keys. This speed is still enhanced in the proposed algorithm LPP-CS by dividing the file into several blocks. Apart from increasing the speed, the implementation of LPP-CS algorithm also makes the computation complex one and increases the strength of security as well as 96.8%. In future, the time spent for encryption and decryption can still be improved by using the concept of Addition chaining. The security level of the algorithm wastested using statistical methods to find the strength of security.

Table 5 Comparison of frequent occurrence.

Methods Explored/ Users	Analysis of Frequent Occurrence					
	Consistency Service	RSA	DES	AES	R2R-CSES	LPP-CS
50 users	9.3	7.4	6.7	4.1	3.6	3.2
100 users	10.4	8.4	7.8	5.8	3.1	2.9
150 users	12.7	9.4	8.3	6.5	4.8	3.6

CONFLICT OF INTEREST

The authors declare they have no conflicts of interest.

Funding Statement

This research received no external funding.

REFERENCES

[1] J. Daemen, V. Rijmen, The Design of Rijndael: AES the Advanced Encryption Standard, Springer, Verlag-Berlin, Heidelberg, 2002.
[2] N. Kofahi, T.F. Al-Somani, K. Al-Zamil, Performance evaluation of three encryption/decryption algorithms, in Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS '03), Cairo, Egypt, 2 (2003), 790–793.
[3] W. Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall, 2005.
[4] P. Paillier, J. Villar, Trading one-wayness against chosen cipher text security in factoring-based encryption, ASIACRYPT, China, 2006, 252–266.
[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, Toward secure and dependable storage services in cloud computing, IEEE Trans. Serv. Comput. 5 (2012), 220–232.
[6] K. Ren, C. Wang, Q. Wang, Security challenges for the public cloud, IEEE Internet Comput. 16 (2012), 69–73.
[7] C. Rong, S.T. Nguyen, M.G. Jaatun, Beyond lightning: a survey on security challenges in cloud computing, Comput. Electr. Eng. 39 (2013), 47–54.
[8] Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, Enabling public auditability and data dynamics for storage security in cloud computing, IEEE Trans. Parallel Distr. Syst. 22 (2011), 847–859.
[9] S. El-etriby, H.S. Abdul-kader, E.M. Mohamed, Modern encryption techniques for cloud computing, in ICCIT, Al-Madinah Al-Munawwarah, Saudi Arabia, 2012, pp. 800–805.
[10] P. Yellapa, C. Narasimham, V. Sreenivas, Data security in cloud using RSA, in 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), IEEE, Tiruchengode, India, 2013, pp. 1–6.

[11] C. Wang, S.M. Chow, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for secure cloud storage, IEEE Trans. Comput. 62 (2013), 362–375.
[12] A.E. Taki El_Deen, Design and implementation of hybrid encryption algorithm, Int. J. Sci. Eng. Res. 4 (2013), 669–673.
[13] U. Naik, V.C. Kotak, Security issues with implementation of RSA and proposed dual security algorithm for cloud computing, IOSR J. Electron. Commun. Eng. (IOSR-JECE), 9 (2014), 43–47.
[14] S.A. Khan, Design and analysis of playfair ciphers with different matrix sizes, Int. J. Comput. Netw. Technol. 3 (2015), 117–122.
[15] I. Jahan, M. Asif, L.J. Rozario, Improved RSA cryptosystem based on the study of number theory and public key cryptosystems, Am. J. Eng. Res. 4 (2015), 143–149.
[16] N. Khanezaei, Z.M. Hanapi, A framework based on RSA and AES encryption algorithms for cloud computing services, 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), IEEE, Kuala Lumpur, Malaysia, 2016, pp. 58–62.
[17] X. Chen, J. Li, J. Weng, J. Ma, W. Lou, Verifiable computation over large database with incremental updates, IEEE Trans. Comput. 65 (2016), 3184–3195.
[18] N. Sengupta, Designing of hybrid RSA encryption algorithm for cloud security, Int. J. Innov. Res. Comput. Commun. Eng. 3 (2015), 4146–4152.
[19] X. Chen, J. Li, X. Huang, J. Ma, W. Lou, New publicly verifiable databases with efficient updates, IEEE Trans. Depend. Secure Comput. 12 (2015), 546–556.
[20] H. Tian, Y. Chen, C.C. Chang, H. Jiang, Y. Huang, Y. Chen, J. Liu, Dynamic-hash-table based public auditing for secure cloud storage, IEEE Trans. Serv. Comput. 10 (2016), pp. 1–14.
[21] H. Zang Xiaojun, X. Chunxiang, Z. Yuan, Insecurity of a public proof of cloud storage from lattice assumption, Chin. J. Electron. 26 (2017), 88–92.
[22] S. Nagaraj, G.S.V.P. Raju, V. Srinadth, Data encryption and authentication using public key approach, Procedia Comput. Sci. 48 (2015), 126–132.
[23] L. Wouter, G. Alpár, J.-H. Hoepman, Fast revocation of attribute-based credentials for both users and verifiers, Comput. Sec. 67 (2017), 308–323.
[24] Z. Fu, K. Ren, J. Shu, X. Sun, Enabling personalized search over encrypted outsourced data with efficiency improvement, IEEE Trans. Parallel Distr. Syst. 27 (2016), 2546–2559.