An Overview of Data Security Algorithms in Cloud Computing

Dr. D. I. George Amalarethinam [1†] and S. Edel Josephine Rajakumari [2††],

[1]Bursar & Director (MCA), Associate Professor, [2]Research Scholar
PG & Research Department of Computer Science
Jamal Mohamed College (Autonomous), Affiliated to Bharathidasan University,
Tiruchirappalli – 620020, Tamil Nadu, India.

Summary

Cloud Computing is one of the current research areas in computer science. Recently, Cloud is the buzz word used everywhere in IT industries; It introduced the notion of 'pay as you use' and revolutionized developments in IT. The rapid growth of modernized cloud computing leads to 24×7 accessing of e-resources from anywhere at any time. It offers storage as a service where users' data can be stored on a cloud which is managed by a third party who is called Cloud Service Provider (CSP). Since users' data are managed by a third party, it must be encrypted ensuring confidentiality and privacy of the data. There are different types of cryptographic algorithms used for cloud security; in this article, the algorithms and their security measures are discussed.

Key words:
cloud, resources, services, applications, security.

1. Introduction

Cloud computing is a model that enables on-demand network access to computing resources like network, server, storage, applications and services based on pay as you go strategy [1]. It offers numerous benefits to the IT industry through optimized usage of resources as services when there is a demand. It has five significant characteristics, four deployment models and three service models. The Cloud clients should have an account with a CSP and can avail the cloud services with internet access. Despite, Cloud offers more benefits to the realm, there are some security challenges that need to be addressed [2]. In this paper, existing cryptographic algorithms that are used to encrypt the cloud data are discussed.

Cryptography means protecting data or information from unauthorized users by encoding the data or information into an illegible format; It is the process of converting a plaintext (original text) into a ciphertext (converted text) and vice versa. In Computer networks, some cryptographic algorithms are developed and used for protected communication. Those algorithms can be used to secure cloud data too. The cryptographic algorithms are classified as symmetric and asymmetric algorithms. The commonly used security algorithms are: DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA (Rivest, Shamir and Adleman), Blowfish, Homomorphic encryption, Honey encryption, etc.

2. Cloud Security

The migration of data from client machine to cloud entails security of the migrated data. The Cloud Service Providers offer storage resource as a service to the clients to store their data which can be accessed from everywhere. As the data are outsourced to CSP's servers for storage purpose, there is a need for providing security of the stored data. The Existing security algorithms are used for securing cloud data discussed in the section.

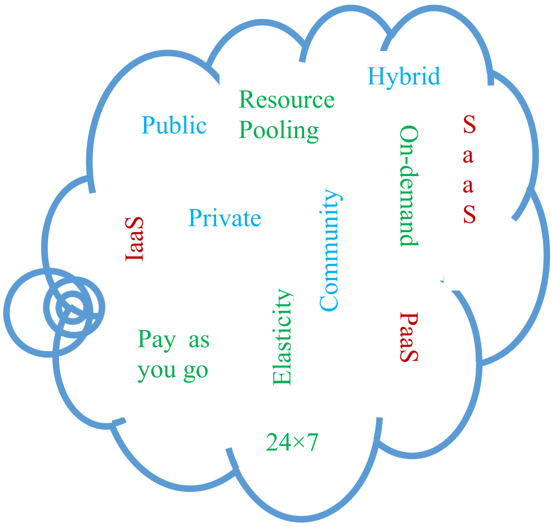

Fig. 1 Cloud Computing

2.1 DES

DES is a symmetric key algorithm where the same key is used for encryption and decryption processes. It is a block-cipher algorithm which means the encryption and decryption taking place in terms of a block of text rather than a bit. DES takes 64 bits (8 bytes) block size that fits a combination of zeros and ones. The key length used in DES

Manuscript received May 5, 2023
Manuscript revised May 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.5.9

Table 1: Cryptographic Algorithms

S. No.	Algorithm	Developed By	Type of Algorithm	Block Size	Key Size	Rounds
1	Data Encryption Standard (DES)	IBM	Symmetric	64 bits	56 bits (+8 parity bits)	16
2	Triple Data Encryption Standard (TDES)	-	Symmetric	64 bits	168, 112 or 56 bits	48
3	Advanced Encryption Standard (AES)	Vincent Rijmen, Joan Daemen	Symmetric	128 bits	128, 192 or 256 bits	10, 12 or 14
4	Blowfish	Bruce Schneier	Symmetric	64 bits	32 – 448 bits	16
5	RSA	Ron Rivest, Adi Shamir, and Leonard Adleman	Asymmetric	-	1,024 to 4,096 bits	1

also a 64-bit key; but one byte is used for parity checking; There are 2^56 possibilities of keys can be generated.

2.2 3DES

Triple DES is a symmetric key block-cipher algorithm in which DES algorithm is applied three times to each block of data thus offering greater security to the cloud data. There are three keys of different sizes used in this algorithm such as 168 (56+56+56), 112 (56+56) and 56 to the 64 bits of data block. 3DES is an extended version of DES algorithm.

2.3 AES

AES also a symmetric cryptographic algorithm which uses three different key sizes viz. 128-bit, 192 bit and 256 bits on 128 bits of data block. It is stronger and faster than Triple DES. AES uses larger key size than DES. Its implementation is very easy and faster than DES. AES is more secure than DES and 3DES.

2.4 Blowfish

It is a symmetric key block-cipher algorithm and is applied to 64 bits of data block. The key sizes range from 32 bits to 448 bits. The algorithm is executed in 16 rounds; and it is faster than DES. It is swift, succinct, simple and secure algorithm.

2.5 RSA

It is an asymmetric algorithm where two different keys are used for encryption and decryption; a public key is used for encryption and a private key is used for decryption. The algorithm can be used for both confidentiality and authenticity. It is considered as the strongest encryption algorithm in data security.

2.6 Homomorphic Encryption

While the other security algorithms allow the cloud users to encrypt their data before storing it in the cloud, Homomorphic encryption allows to perform computations and search operation on the encrypted data without decrypting it; Privacy is preserved using this algorithm. Functions of Homomorphic encryption [3]: Key generation, Encryption, Decryption and Evaluation.

3. Literature Review

Vishwanath S. Mahalle et. al. [4] proposed a secure Hybrid Algorithm (RSA & AES). The major advantage of the algorithm is System timing is used for key generation. In this algorithm, public key is used for encryption. Private and Secret keys are used for decryption. This algorithm involves secure uploading/downloading of data to/from the cloud and secure sharing of public, private and secret keys. The proposed algorithm was implemented in EyeOS.

D.I. George Amalarethinam et. al. [5] introduced an enhanced RSA algorithm with singly even magic rectangle. The uniqueness of the algorithms is that there are no values repeated in the ciphertext even there exists multiple occurrences of the same character. It is also proved that the randomness is increased using the algorithm.

Nasrin Khanezaei et. al. [6] proposed a framework that is a combination of encryption methods using RSA and AES which diminishes the communication time between cloud storage and user.

Er. Ashima et. al. [7] discussed the existing security algorithms such as DES, AES, Triple DES, Blowfish, IDEA, RSA and Diffie-Hellman key exchange. They suggested that the existing security algorithms are not strong so that enhanced cloud security algorithms are to be developed.

Srinivasan Nagaraj et. al. [8] proposed a key generation method that is highly secure and increases randomness. They proved that confidentiality is achieved with this algorithm. It is also economical when compared to other public key cryptographic algorithms.

D.I. George Amalarethinam et. al. [9] asserted that Cryptographic strength is based on the secrecy of the key; longer keys are generally harder to guess or find. Also, they have made comparison on features of symmetric and asymmetric cryptosystem. It is suggested that combination of Enhanced RSA and ElGamal algorithms provide higher level of data security.

Debasis Das et. al. [10] proposed a hybrid encryption algorithm by which they proved that Multi Party Computation (MPC) provides both confidentiality as well as integrity which is much better than FHE (Fully Homomorphic Encryption).

Ibtissam Ennajjar et. al. [11] proposed Ciphertext Policy – Attribute Based Encryption (CP-ABE) and suggested that the proposed algorithm can be extended as KP, HABE, HASBE and MAABE algorithms.

Priyadarshini Patil et. al. [12] made evaluation of different security algorithms like DES, 3DES, AES, RSA and Blowfish with respect to encryption and decryption time, memory used, avalanche effect, entropy and number of bits required for encoding. Each algorithm has its own unique strength according to the mentioned metrics.

Akashdeep et. al. [13] discussed Symmetric and Asymmetric cryptographic algorithms in the paper. Also, they have compared symmetric encryption algorithms with respect to encryption and encoding time and found that AES is the best algorithm for key encryption and MD5 is the best for encoding files.

Manish M Potey et. al. [14] proposed a data security solution where users can store their data as encrypted using FHE (Fully Homomorphic Encryption) in DynamoDB of the public cloud AWS (Amazon Web Services) and can perform computations on the encrypted data without decrypting it. It is recommended that reducing the size of cipher text leads to efficient data processing. Also, various algorithms for searching and querying on encrypted data under Fully Homomorphic Encryption (FHE) scheme can be developed in future.

Kamal Benzekki et. al. [15] proposed a multi-cloud architecture of N distributed servers to repartition the data achieving FHE (Fully Homomorphic Encryption) for the security of data stored in cloud.

Ihsan Jabbar et. al. [16] analyzed PHE (Partially Homomorphic Encryption) and FHE (Fully Homomorphic Encryption) schemes and inferred that PHE algorithms such as RSA and Pailier are not efficient, because they perform only one operation either addition or multiplication on the encrypted data. They found that FHE is the best solution to protect the client data since it performs arbitrary calculations on the cipher text. Thus, SDC scheme is considered, the most efficient to secure data stored in cloud.

Priya G et. al. [17] compared the security algorithms used in cloud computing with the following parameters: size, initial vector size, security, memory usage, scalability, information encryption capacity, execution time and key used.

Nasarul Islam K.V. et. al. [18] enlisted the challenges of Cloud computing and compared the encryption algorithms such as AES, DES, RSA and homomorphic algorithms. They concluded that Homomorphic algorithm provides greater security than AES, DES and RSA algorithms.

Vikas K. Soman et. al. [19] proposed a hybrid data security algorithm which involves ECDSA, SHA 256 and AES algorithms. They have suggested enhancements on their algorithm as comparison of different hybrid cryptographic algorithm for data security in cloud should be performed and Efficiency analysis of different large file size with these algorithms to be carried out.

S. Rajendirakumar et. al. [20] made a comparative study among symmetric, asymmetric and hashing algorithms with respect to execution time and produced results. The results proved that AES took less time to execute cloud data whereas RSA took more time to execute the same. They recommended that, new efficient algorithms can be developed by combining Diffie-Hellman and MD5 algorithms.

D.I. George Amalarethinam et. al. [21] compared symmetric key algorithms such as AES, DES and Blowfish and found that the Blowfish algorithm is the best algorithm for data encryption because of its speed.

Sarah Shihab Hamad et. al. [22] proposed a FHE scheme based on a prime modular operation that encrypts the message character by character by using a prime secret key without converting that character into a binary format. They proved that the proposed SAM scheme is very fast at execution compared to DGHV and SDC.

K.V. Pradeep et. al. [23] proposed an efficient framework for sharing a file in a secure manner that preserves privacy using asymmetric key distribution management in Cloud environment. They have compared

RSA algorithm with EIGamal and Pailier algorithms and found that RSA is better than EIGamal and Pailier with respect to time and computational speed.

Naveen N et. al. [24] proposed a multi-layer encryption approach to the security of Cloud data. In this work, the data owner encrypts the file twice before uploading it to the cloud server. The user requesting the cloud data is authenticated twice for stronger authentication. The use of security algorithms AES (symmetric) and RSA (asymmetric) provides multi-layer encryption of cloud data hence security and privacy are preserved using this approach.

Min Zhao E et. al. [25] analysed Single Homomorphic Encryption (SHE) algorithms such as Hill Cipher, RSA, EIGamal and Pailier and compared encryption and decryption time of four algorithms. FHE algorithms such as Gentry's homomorphic encryption (based on ideal lattice), DGHV (based on Integer), BGV (based on RLWE), GSW13 (based on approximate eigenvectors), Multi-key FHE (based on NTRU) are also analysed and compared their performance. Based on the analysis, it is suggested that the cipher text expansion rate and computational complexity should be reduced; and, RSA and NTRU homomorphic schemes need improvement for better performance.

Madhu Agarwal Agnihotri et. al. [26] proposed a homomorphic encryption method and recommended HE Schemes for sorting encrypted data. They have found that Lazy sort technique, a FHE based two stage sorting technique gives better performance on FHE data comparing to partition and comparison sort.

Utkarsh Singh et. al. [27] proposed an image segmentation method for secure image partitioning for cloud services by using OCR (Optical Character Reader) and Cloud Analyst.

Vinay Poduval et. al. [28] suggested that higher level of security can be provided using Hybrid cryptography. Image steganography is used in their proposed system.

4. Observations

When there is a technology growth, challenges associated with the technology are also increasingly grown. Cloud computing offers computing resources like network, server, storage as services so that ubiquitous computing is possible everywhere in today's world. Cloud follows multi-tenancy concept that offers an advantage of computing at lower cost, it may cause security issues, since a single instance of a resource is shared by multiple tenants. When the data owners store their data in cloud, they encrypt their data before storing it in the cloud using cryptographic algorithms like DES, 3DES, AES, RSA, etc. The algorithms' specifications, advantages and limitations are given in the Table 2.

When the data is accessed by the users of a cloud, the confidentiality of the data must be maintained. For this purpose, many cryptographic algorithms were developed and used. In this paper, the different algorithms such as DES, 3DES, AES, RSA, Blowfish and Homomorphic algorithms were discussed. Among the 6 algorithms, RSA is considered as the highly secure algorithm because the computation is based on large prime numbers. Based upon the Literature review, it is found that Homomorphic encryption is considered to be the efficient encryption method since computations can be performed on the encrypted data without converting it to the original data. Different types of homomorphic encryption algorithms are existing in the present scenario; the algorithms can be enhanced by appending additional features to them or minimizing the time and computational complexity of the algorithms. Also, it is found that Hybrid Data Security algorithms are more efficient than the existing security algorithms since every algorithm has its own strong mathematical computations and randomness.

Table 2: Findings and Limitations in Data Security Algorithms

Authors	Title of the Paper	Findings and Limitations
Vishwanath S. Mahalle & Aniket Shahade [4]	Enhancing the Data Security in Cloud by implementing Hybrid (RSA & AES) Encryption Algorithm (2014)	• Secure Hybrid Encryption Algorithm (RSA & AES). • System timing is used for key generation so as randomness is increased.

D.I. George Amalarethinam, J.Sai Geetha & K.Mani [5]	Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting (2014)	• An enhanced RSA algorithm with singly even magic rectangle. • No values repeated in the ciphertext even there exists multiple occurrences of the same character so as randomness is increased.
Nasrin Khanezaei & Zurina Mohd Hanapi [6]	A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services (2014)	• A framework that is a combination of RSA and AES. • Reduces the communication time between cloud storage and user.
Er. Ashima Pansotra & Er. Simar Preet Singh [7]	Cloud Security Algorithms (2015)	• discussed DES, AES, Triple DES, Blowfish, IDEA, RSA and Diffie-Hellman key exchange. • Enhanced cryptographic algorithms are to be enhanced.
Srinivasan Nagaraj, Dr.G.S.V.P.Raju & V.Srinadth [8]	Data Encryption and Authentication Using Public Key Approach (2015)	• A Key generation algorithm which increases randomness. • Confidentiality is achieved. • Economical compared to other public key cryptographic algorithms.
Dr. D. I. George Amalarethinam & J. Sai Geetha [9]	A Survey on Secured Communication with High Speed and Public Key Cryptography (2016)	• Cryptographic strength is based on the secrecy of the key • Longer keys are generally harder to guess or find. • combination of Enhanced RSA and ElGamal algorithms provide higher level of data security.
Bhandari A., Gupta A. & Das D. [10]	Secure algorithm for cloud computing and its applications (2016)	• A hybrid encryption algorithm • Multi Party Computation (MPC) provides both confidentiality and integrity • Better than FHE.
Ibtissam Ennajjar, Youness Tabii & Abdelhamid Benkaddour [11]	An Enhanced Approach for Data Sharing Security in Cloud Computing (2016)	• proposed Ciphertext Policy – Attribute Based Encryption (CP-ABE).
Priyadarshini Patil, Prashant Narayankar, Narayan D G & Meena S M [12]	A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish (2016)	• evaluated the different security algorithms: DES, 3DES, AES, RSA and Blowfish with respect to encryption and decryption time, memory used, avalanche effect, entropy and number of bits required for encoding.
Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi & Hanumat Sastry [13]	Security Algorithms for Cloud Computing (2016)	• AES is the best algorithm for key encryption and MD5 is the best algorithm for encoding files.
Manish M Potey, Dr C A Dhote & Deepak H Sharma [14]	Homomorphic Encryption for Security of Cloud Data (2016)	• Reducing the size of cipher text leads to efficient data processing.
Kamal Benzekki, Abdeslam El Fergougui, Abdelbaki El Belrhiti El Alaoui [15]	A Secure Cloud Computing Architecture Using Homomorphic Encryption (2016)	• A multi-cloud architecture of N distributed servers to repartition the data achieving FHE for the security of data stored in cloud.
Ihsan Jabbar & Saad Najim [16]	Using Fully Homomorphic Encryption to Secure Cloud Computing (2016)	• FHE is the best solution to protect the client data since it performs arbitrary calculations on the cipher text.
Priya G, Lawanya Shri M, Benjula Anbu Malar M.B., Santhi K & Deepa M [17]	Security Algorithms in Cloud Computing: A Review (2017)	• compared the security algorithms with the following parameters: size, initial vector size, security, memory usage, scalability, information encryption capacity, execution time and key used.
Nasarul Islam.K.V & Mohamed Riyas.K.V [18]	Analysis of Various Encryption Algorithms in Cloud Computing (2017)	• compared the encryption algorithms such as AES, DES, RSA and homomorphic algorithms. • Homomorphic algorithm provides greater security than AES, DES and RSA algorithms.

Vikas K.Soman & Natarajan V [19]	An Enhanced hybrid Data Security Algorithm for Cloud (2017)	• proposed a hybrid data security algorithm which involves ECDSA, SHA 256 and AES algorithms.
S. Rajendirakumar & A. Marimuthu [20]	Cryptographic Algorithms used in Cloud Computing – An Analysis and Comparison (2018)	• made comparison among symmetric, asymmetric and hashing algorithms with respect to execution time. • AES took less time to execute cloud data whereas RSA took more time to execute the same.
D.I. George Amalarethinam & H.M. Leena [21]	A Comparative Study on various Symmetric Key Algorithms for enhancing Data Security in Cloud Environment (2018)	• compared symmetric key algorithms such as AES, DES and Blowfish. • Blowfish algorithm is the best algorithm for data encryption because of its speed.
Sarah Shihab Hamad & Ali Makki Sagheer [22]	Design of Fully Homomorphic Encryption by Prime Modular Operation (2018)	• proposed a FHE scheme based on a prime modular operation. • proposed SAM scheme is very fast at execution compared to DGHV and SDC.
K.V.Pradeep, V.Vijayakumar & V.Subramaniyaswamy [23]	An Efficient Framework for sharing a file in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment (2019)	• proposed an efficient framework for sharing a file in a secure manner that preserves privacy. • compared RSA algorithm with EIGamal and Pailier algorithms • RSA is better than EIGamal and Pailier with respect to time and computational speed.
Naveen N & K.Thippeswamy [24]	Security and Privacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments (2019)	• proposed a multi-layer encryption approach to the security of Cloud data. • AES (symmetric) and RSA (asymmetric) provides multi-layer encryption. • security and privacy are preserved using this approach.
Min Zhao E & Yang Gen [25]	Homomorphic Encryption Technology for Cloud Computing (2019)	• compared encryption and decryption time of four algorithms: Hill Cipher, RSA, EIGamal and Pailier. • suggested that the cipher text expansion rate and computational complexity should be reduced. • RSA and NTRU homomorphic schemes need improvement for better performance.
Madhu Agarwal Agnihotri & Mahua Pal [26]	Homomorphic Encryption Method for Business Data Security in Cloud (2020)	• proposed a homomorphic encryption method. • recommended HE Schemes for sorting encrypted data. • Lazy sort technique, gives better performance on FHE data than partition and comparison sort.
Utkarsh Singh, Abhay Tiwari & Shruti Sharma [27]	Data Security in Cloud Computing (2020)	• proposed an image segmentation method for secure image partitioning for cloud services by using OCR (Optical Character Reader) and Cloud Analyst.
Vinay Poduval, Ashish Koul, Daniel Rebello, Karunesh Bhat & Revati M. Wahul [28]	Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography (2020)	• suggested that higher level of security can be provided using Hybrid cryptography.

5. Problem Definition

Cloud offers IT resources such as storage, network, server and applications as services to its consumers, delivered through internet based on pay-as-you-go method. Storage is a major cloud service adopted by most of the companies and business organizations. As companies migrate more data and applications to the cloud, IT professionals remain concerned about security, governance, and compliance issues when their content is stored in the cloud. The existing security policies and algorithms are not sufficiently providing stronger security to the data stored in the cloud. Hence, enhanced security algorithms are to be designed to provide robust security than the existing algorithms for the cloud environment.

6. Future Work

It is well known that cryptographic algorithms involve comprehensive mathematical computations to make it stronger than any other algorithms. As the existing cloud security algorithms are need to be enhanced, evolutionary algorithms like differential evolution can be used for Key Generation. The encryption process can be enhanced by using the Magic Triangle concept [5]. Further, the keys generated by differential evolution algorithm and the encryption by magic triangle can be applied to the Blowfish algorithm [21]. Finally, a framework can be designed by encompassing the proposed algorithms, which could be a highly secure way for providing data security in cloud computing.

7. Conclusion

Security is the major challenge that needs to be rectified or improved in Cloud computing. Since users' data are outsourced to third-party CSP, there is a need for data security in cloud. Albeit existing network cryptographic algorithms provide security to the cloud data, improvement is required for stronger security. Every security algorithm has its own advantages and limitations when compared to other algorithms. Cloud computing requires a holistic security approach to provide enhanced security that never be compromised. The future research work can be focused on hybrid data security algorithms and modifying the RSA with arbitrary computations and make it as a FHE algorithm so that RSA would be the most efficient algorithm for securing the cloud data in the future.

References

[1] Peter Mell and Timothy Grance: *The NIST Definition of Cloud Computing.* In: National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication, 14 (2011)

[2] D.I.George Amalarethinam, S.Edel Josephine Rajakumari: *A Survey on Security Challenges in Cloud Computing.* In: Journal of Physical Sciences, ISSN. 2350-0352 (p), vol. 24, pp. 133 – 141 (2019)

[3] Payal V. Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt, Rutvij H. Jhaveri: *Survey of Various Homomorphic Encryption algorithms and Schemes.* In: International Journal of Computer Applications, ISSN. 0975 – 8887, vol. 91 (8) (2014)

[4] Vishwanath S. Mahalle, Aniket Shahade: *Enhancing the Data Security in Cloud by implementing Hybrid (RSA & AES) Encryption Algorithm.* In: IEEE (2014)

[5] D.I. George Amalarethinam. J.Sai Geetha, K.Mani: *Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting.* In: International Journal of Computer Applications, ISSN. 0975 – 8887, vol. 96 (14) (2014)

[6] Nasrin Khanezaei, Zurina Mohd Hanapi: *A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services.* In: IEEE (2014)

[7] Er. Ashima Pansotra, Er. Simar Preet Singh: *Cloud Security Algorithms.* In: International Journal of Security and Its Applications, vol.9 (10), pp.353-360 (2015)

[8] Srinivasan Nagaraj, Dr.G.S.V.P.Raju, V.Srinadth: *Data Encryption and Authentication Using Public Key Approach.* In: Elsevier Procedia Computer Science, 48, pp. 126 – 132 (2015)

[9] D. I. George Amalarethinam, J. Sai Geetha: *A Survey on Secured Communication with High Speed and Public Key Cryptography.* In: International Journal of Scientific and Engineering Research (IJSER), vol. 7 (4), (2016)

[10] Bhandari A., Gupta A., & Das D.: *Secure algorithm for cloud computing and its applications.* In: IEEE (2016)

[11] Ibtissam Ennajjar, Youness Tabii, Abdelhamid Benkaddour: *An Enhanced Approach for Data Sharing Security in Cloud Computing.* In: International Journal of Cloud Computing, vol. 5 (3), (2016)

[12] Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S M: *A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish.* In: Elsevier Procedia Computer Science 78, pp. 617 – 624 (2016)

[13] Akashdeep Bhardwaj, GVB Subrahmanyam, Vinay Avasthi, Hanumat Sastry: *Security Algorithms for Cloud Computing.* In: Elsevier Procedia Computer Science 85, pp. 535 – 542 (2016)

[14] Manish M Potey, Dr C A Dhote, Deepak H Sharma: *Homomorphic Encryption for Security of Cloud Data.* In: Elsevier Procedia Computer Science 79, pp. 175 – 181 (2016)

[15] Kamal Benzekki, Abdeslam El Fergougui, Abdelbaki El Belrhiti El Alaoui: *A Secure Cloud Computing Architecture Using Homomorphic Encryption.* In: International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 7 (2) (2016)

[16] Ihsan Jabbar, Saad Najim: *Using Fully Homomorphic Encryption to Secure Cloud Computing.* In: Internet of Things and Cloud Computing, ISSN. 2376-7715 (p), ISSN. 2376-7731 (o) vol. 4 (2), pp. 13 – 18 (2016)

[17] Priya G, Lawanya Shri M, Benjula Anbu Malar M.B., Santhi K, Deepa M: *Security Algorithms in Cloud Computing: A Review.* In: International Journal of Pure and Applied Mathematics, vol.117 (7), pp. 85 – 92 (2017)

[18] Nasarul Islam K.V, Mohamed Riyas.K.V.: *Analysis of Various Encryption Algorithms in Cloud Computing.* In: International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 6 (7), pp. 90-97 (2017)

[19] Vikas K.Soman, Natarajan V: *An Enhanced hybrid Data Security Algorithm for Cloud.* In: IEEE (2017)

[20] S.Rajendirakumar, Dr.A.Marimuthu: *Cryptographic Algorithms used in Cloud Computing – An Analysis and Comparison.* In: International Journal for Research in Applied Science & Engineering Technology (IJRASET), ISSN. 2321-9653, vol. 6 (1), pp. 2718 – 2728 (2018)

[21] D.I. George Amalarethinam, H.M. Leena: *A Comparative Study on various Symmetric Key Algorithms for enhancing Data Security in Cloud Environment.* In: International Journal of Pure and Applied Mathematics, ISSN. 1311-8080 (P), pp. 85-94 (2018)

[22] Sarah Shihab Hamad, Ali Makki Sagheer: *Design of Fully Homomorphic Encryption by Prime Modular Operation.* In: Telfor Journal, Vol. 10 (2) (2018)

[23] K.V.Pradeep, V.Vijayakumar and V.Subramaniyaswamy: *An Efficient Framework for sharing a file in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment.* In: Journal of Computer Networks and Communications, pp. 1 – 8 (2019)

[24] Naveen N, K.Thippeswamy: *Security and Privacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments.* In: International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN. 2278-3075, vol. 8 (8) (2019)

[25] Min Zhao E, Yang Gen: *Homomorphic Encryption Technology for Cloud Computing.* In: Elsevier Procedia Computer Science 154, pp. 73 – 83 (2019)

[26] Madhu Agarwal Agnihotri, Mahua Pal: *Homomorphic Encryption Method for Business Data Security in Cloud.* In: Our Heritage (UGC CARE Listed Journal), Vol. 68 (8) (2020)

[27] Utkarsh Singh, Abhay Tiwari, Shruti Sharma: *Data Security in Cloud Computing.* In: International Journal of Engineering Applied Sciences and Technology (IJEAST), vol. 4 (10), ISSN. 2455 – 2143, pp. 170 – 173 (2020)

[28] Vinay Poduval, Ashish Koul, Daniel Rebello, Karunesh Bhat, Revati M. Wahul: *Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography*. In: International Journal of Recent Technology and Engineering (IJRTE), vol. 8 (6), ISSN. 2277 – 3878, pp. 665 – 667 (2020)