Journal of the Maharaja Sayajirao University of Baroda
ISSN : 0025-0422

MULTIPATH MULTI ALGORITHM FOR DATA SECURITY AND CHALLENGES MANAGEMENTIN CLOUD COMPUTING

Dr.D.Kavitha, Associate Professor, Dept. of CSA, SPIHER, Chennai.
A.Sandhiya, Research Scholar, Dept. of CSA, SPIHER, Chennai.

ABSTRACT
The cloud platform is an internet-based computing technology. Cloud is a place where all the shared resources, namely software, storage, and information are delivered to customers on demand. In general, the cloud is a computing platform for sharing and transferring resources, which include software, applications, and business works. The security issue is being a big concern as the security threats are increasing immensely, that many organizations have faced at present. Many encrypting techniques and splitting techniques were used. In existing a distribution storage, PSOS (Proficient Security Over Distributed Storage) were used for security purpose that divide the data into two parts which is not enough for securing the data. Here, the proposal uses a Multipath Multi-Algorithm (MPMA) for a distributed storage. MPMA divides the information into several parts, for decryption it uses various algorithms, making it tough for the attackers to encrypt or crash the information.

Keywords: Cloud computing, Data Encryption, PSOS, Security Techniques

I. INTRODUCTION
Cloud is a virtual pool where security, Integrity, Authentication, and Privacy are essential concerns for both Cloud providers and consumers as well. PSOS is an existing algorithm used for security purposes. In PSOS (Proficient Security Over Distributed Storage) the data is partitioned into two parts (decrypted) and stored in the server [1,2,15].
Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [3], [4] are the service providers. SaaS offers service to clients, as an instance, the virtual work area, webmail, and the program interface Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [3], [4] are the service providers. SaaS offers service to clients, as an instance, the virtual work area, webmail, and the program interface. The PaaS provides a stage for using PL (programming language), administrations, libraries, and varied process. IaaS offers online administrations to clients, as an instance, servers, load balancers, and other computing assets. Because of these reasons nowadays businesses, organization, and individual users are moving their information to the cloud.
Various models of cloud, namely privacy, public, hybrid, and community cloud are outlined [5] to produce several services equivalent to infrastructure, software, and others.
Data security may be a crucial concern, whereas transferring information over the system having numerous solutions projected in the literature. Be that as it may, cryptography is one among the principal ways used to encode the data utilizing either a symmetric key or asymmetric key. The asymmetric code is counted exceptionally secure as encoding and decoding using different keys. The key generation method of asymmetric key consumes a large amount of energy and area [6]. Existing proposals have each positive and negatives, for example, Advanced encoding standard (AES) may be a high-security technique used for encoding [7]. Also, the Shamir Secret Sharing theme is employed for encoding [8]. In [9] sensitive information is encrypted by taking XOR with a random number, split, and distributed over 2 clouds.
In [10] the author uses a hybrid technique equivalent to Advanced encoding Standard (AES), Rivest, Shamir Adleman (RSA), Blowfish to secure information. Homomorphic encoding (FHE) is utilized to encode data and so encrypted data is distributed over multi-cloud [11]. In [7] to secure information, AES is employed in combination with MD5, however, there is a chance of a cache-based timing attack on AES [12]. There are possibilities of Biclique attacks on AES, as proved in [13]. Another approach to firmly store/transmit data is in part data into equal components and store it on multi-cloud. To access total information, split parts are mixed. The parting data on multi-cloud

improves security in such the simplest way that though an aggressor gain admittance to a part of the information should still be unable to access the complete information [14].

PSOS CONTRIBUTION

PSOS is an algorithmic technique used to overcome the data security issues over multi cloud.

- A proficient and steady information storage technique has been used previously that distributes sensible users' records among different cloud servers to keep away from any type of attack or vulnerability.
- Also, a mathematical analysis has been evolved and provided together with encryption and decryption algorithms to encrypt and decrypt sensitive in addition to ordinary data. The previous method has been analyzed for security in opposition to numerous recognized attack to evaluate its security [1].

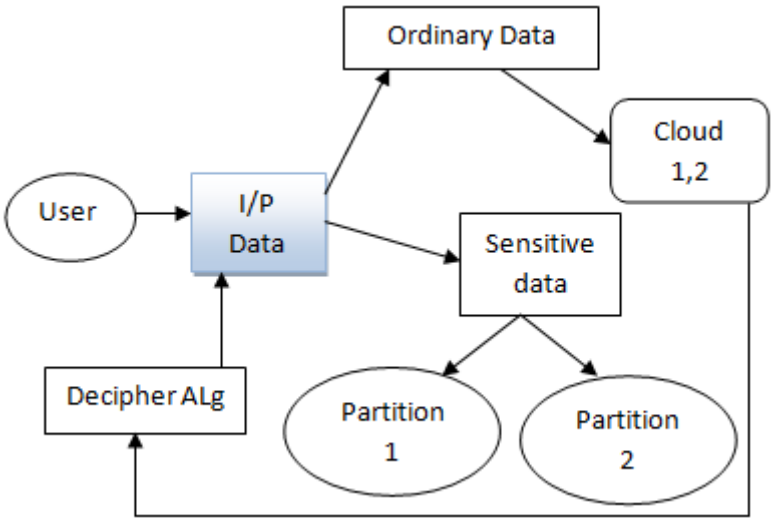


Fig 1. PSOS (Proficient Security Over Distributed Storage)

The method has additionally been analyzed for computation and communication overhead in case of both sensible as well as ordinary data to evaluate its complexity.A comparative evaluation of the previous method has been provided by AES, STRRNS, RFDA, and SA-DES in terms of computation time each for sensitivedata and the overall encipher/decipher time.

In previous PSOS algorithmdivisions the data into two categories; ordinary and sensitive.Here the ordinary data is uploaded directly to the multi-cloud.Whereas, the sensitive data are further divided into two parts and uploaded. But the partition is not enough as the attackers can easily decrypt the two partioned and intrude the data by performing several attacks such as key attack, pollution attacks, chosen ciphertext attack, and known plain text attack.

The rest of the paper is divided as follows: section 1 introduction, section 2discusses the Literature Review, section 3 elaborates the SystemArchitecture of the proposed MPMA, section 4 describesthe proposed MPMA technique. In section 5 an step-by-step algorithm has been discussed. In section 6experimental results arecompared. In section 7 security analysis is explained, and in section 8 the paper has been concluded.

The below algorithm defines as follows:

- At first, an input user data are produced for cloud storage.
- Then, the data is differentiated as common and sensitive data which is defined as C_dS_d.
- When an input data are common then the data is simply encrypted and stored in the cloud database.
- If the data is a sensitive data, then the data DS_n-data splitup for n number of times using various algorithmic techniques.

- Then the sensitive encrypted data is stored in different cloud.
- Then, D_{cc} is used to detect and block chosen cipher text attack and any other vulnerable attacks.

Algorithm 1 Algorithm formulti part multi algorithm(MPMA)

Input: C_dS_d//common and sensitive data
Output: secure data storage
initialization:
while(I_d)//input data
If(I_d=C_d)then//input data is common
DS_n//data splitup for n times
E_d//encrypt data
C_s//stored in different clouds
Else if(I_d=S_d)then//input data is sensitive data
DS_n//data splitup for n times
D_cD_p//different cryptography for different part
C_s//stored in different clouds
Endif
D_{cc}//detect and block chosen cipher text attack
Endwhile

I_d - input data
C_d – common data
E_d - Encrypt data
S_d - sensitive data
D_cD_p- Different cryptography for different part
D_{cc} - detect and block cipher text attack

II. MULTI-PATH MULTI-ALGORITHM (MPMA)

Cloud storage is a virtual pool that provides astorage place for the users to store their records or data's.Also, uploading data on multi-cloud does not mean that the data is safe and secure. There is a requirement for an effective encryption algorithm,whichdelivers high security with less computational time. Various encryption techniques are proposed to secure data over the cloud as discussed in above. But,each and every proposal is not generic and secure and every area has its own pros and cons.

The proposed MPMA method is related to symmetric key encryption to enhance the confidentiality of the data even if the data is uploaded in parts on various clouds. As the previous method here the data is partitioned as a normal data and sensitive data.

The method uploads sensitive data on a multi-cloud to protect it from unauthorized access as well as in case of any undesirable situation, all data must not be at a single location.

Contribution Of MPMA:

- The normal data is encrypted and uploaded in the cloud database.
- Whereas, the sensitive data is more sensible, so two parts are not enough. So, in MPMA the sensitive data is partitioned as five parts or more.
- A random division of the users' sensitive data is made.
- Then, each part is encrypted by a cryptographic technique to enhance the security.

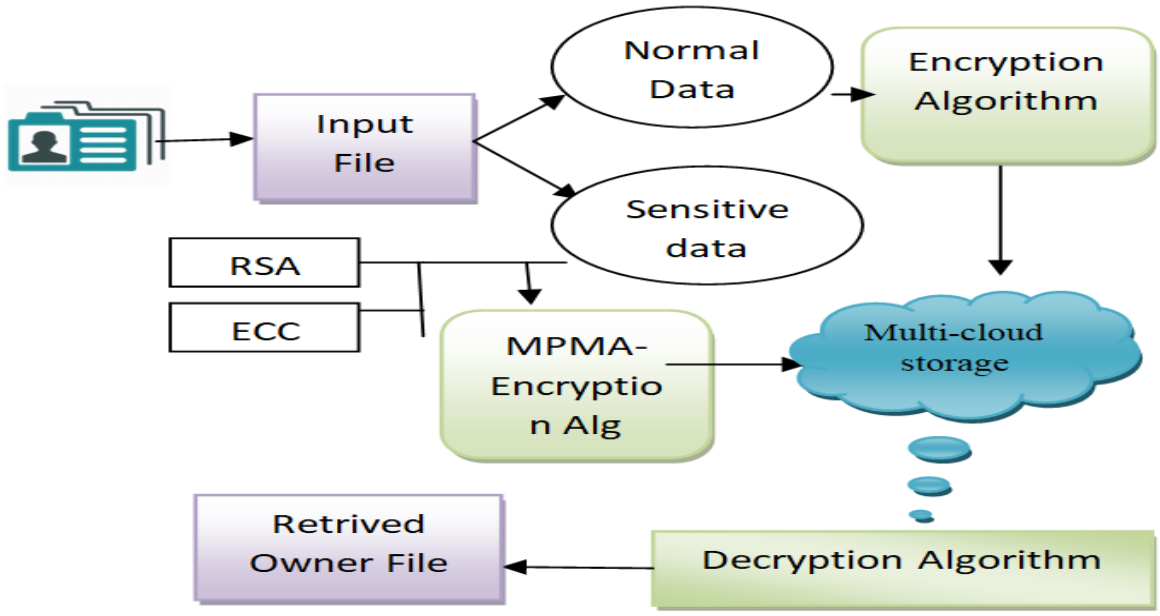


Figure 2. Multi-path Multi-Algorithm Architecture

In the method a key generation technique and a splitter algorithm are used for securing the data.
The working of a the proposed system can be listed as two phases; Data distribution among multi-cloud, and collecting and merging data from multi-cloud. On data distribution stage, private data are split into random parts to store each part on a different cloud ensuring security in case one cloud gets compromised.
In collecting and merging phase, the chunks of multi-cloud are recollectedand merged to obtain the plain text. The working of the proposedMPMA approach is divided into different parts including; Random Cryptographic Key Generation, Algorithm splitter, random encryption and decryption algorithm. The key generation used to generate keys for symmetric encryption to enhance the security of the data to be stored in the cloud. A splitting algorithm to divide the sensitive data into random parts, and use cryptographic encryption techniques and decryption algorithms. The encryption and decryption algorithm helps to encrypt data while uploading and decrypt it back the data owner wants to access the data.

1. RANDOM CRYPTOGRAPHIC KEY GENERATION

The cryptography key generation process uses a random cryptography algorithm generator to generate a random algorithm and calculates its complement.

2. ALGORITHM SPLITTER

Before encrypting the data a client describes the category of data, whether thedata areprivate and sensitive type or Normal data is encrypted using encryption algorithm. After encryption, the encrypted text is uploaded on a single cloud. While sensitive data is divided into random parts. The split parts are encrypted separately with the various encryption algorithms. Then these

3. MULTI ENCRYPTION ALGORITHM AND DECRYPTION ALGORITHM

Encryption Algorithm :In the encryption stage of normal data, a single conversion, encryption takes place and stored in the cloud.The sensitive data uses several cryptography algorithms such as ECC, RSA and several other algorithms for enciphering. The total time required to transform a plaintext intoa ciphertext is named as encryption time.Systems with hard and experienced security need more

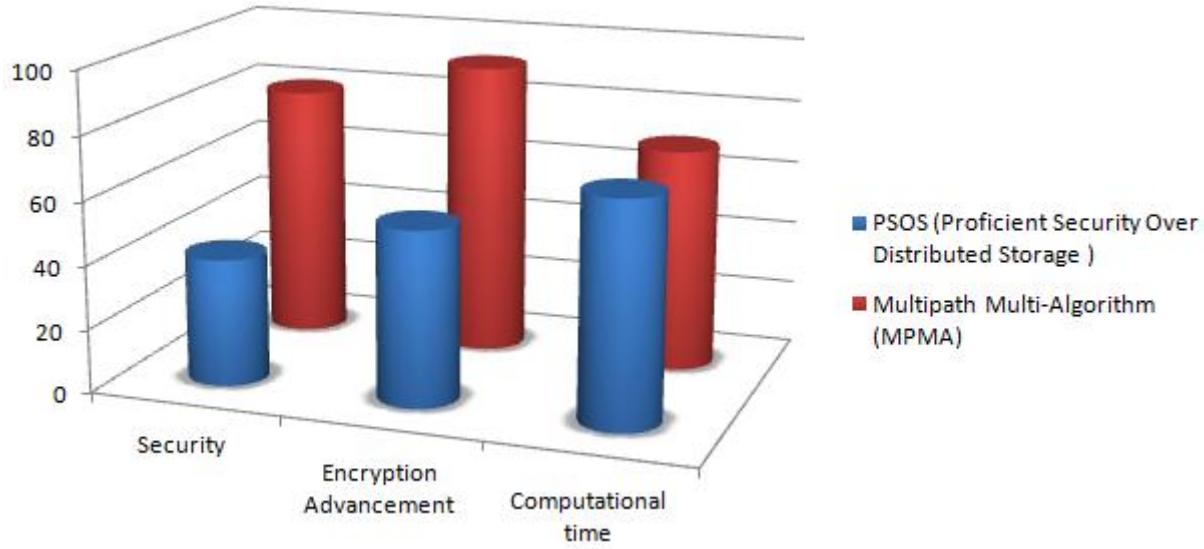
time for converting a plain datainto a cipher data as the encryption process performs harder computation.

Decryption Algorithm:In the decryption, method ciphertext is converted into normaltext. The conversion process of multiple ciphertext into the normal textof MPMA is initiated.At last normal plain text is obtained. The whole time used to convert cipher text into plain text is called as decryption time. It takes less time for a normal data to be decrypted, whereas the decryption time for sensitive data is more than a normal data.

Computational time: The computational time is an important performance analysis for an encryption approach that delivers the entire number of operations and how many times a certain operation is performedatone transaction of a protocol.Computation time is the amount of time taken byan algorithm to complete a certainnumber of computations totally.

III. RESULT ANALYSIS

In the result analysis, a comparison of the existing model and the proposed model is made. And the model proposed is proved be the best implementation.



Graph 1. PSOS vs MPMA.

Here in graph 1, a comparison between the previous model (PSOS) and the proposed model (MPMA) is made. Where the proposed model has proven to be higher in overall performance, security, encryption enhancement, and computational time.

IV. CONCLUSION

The challenges faced for cloud security are being increased day by day. There are many algorithms proposed to solve the security issues in cloud. But the security isn't resolved yet. PSOS (Proficient Security Over Distributed Storage)is an effective distribution technique used in cloud during encryption. In the proposed system the method used many advancements compared to the other algorithms. MPMA is a multiple path multi algorithm were the normal data and sensitive data are differentiated first. Then. The sensitive data is furthermore encrypted with a random number of parts using cryptography algorithms. This encryption technique provides more security for user data stored in cloud database. Where a safe data can be retrieved by the user without any attack or harm.

The challenges of using NN-based SEI algorithms in IoT networks used in existing have been discussed, as well as design considerations and previous algorithm improvements to make using such algorithms feasible have been discussed.

REFERENCES

[1] F. Shahid, H. Ashraf, A. Ghani, S. A. K. Ghayyur, S. Shamshirband and E. Salwana, "PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud," in IEEE Access, vol. 8, pp. 118285-118298, 2020, doi: 10.1109/ACCESS.2020.3004433.

[2] R. Manoj, A. Alsadoon, P. W. C. Prasad, N. Costadopoulos and S. Ali, "Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud," 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), San Francisco, CA, 2017, pp. 185-190, doi: 10.1109/MobileCloud.2017.38.

[3] P. P. Kumar, P. S. Kumar, and P. J. A. Alphonse, ``Attribute based encryptionin cloud computing: A survey, gap analysis, and future directions,"*J. Netw. Comput. Appl.*, vol. 108, pp. 37_52, Apr. 2018, doi: 10.1016/j.jnca.2018.02.009.

[4] A. Botta, W. de Donato, V. Persico, and A. Pescapé, ``Integration of cloudcomputing and Internet of Things: A survey," *Future Gener. Comput. Syst.*,vol. 56, pp. 684_700, Mar. 2016.

[5] S. Ramgovind, M. M. Eloff, and E. Smith, ``The management of securityin cloud computing," in *Proc. Inf. Secur. South Africa*, Aug. 2010, pp. 1_7.

[6] S. Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, ``Contentbased double encryption algorithm using symmetric key cryptography,"*Procedia Comput. Sci.*, vol. 57, pp. 1228_1234, Jan. 2015.

[7] R. F. Olanrewaju, B. U. I. Khan, A. Baba, R. N. Mir, and S. A. Lone,``RFDA: Reliable framework for data administration based on split-mergepolicy," in *Proc. SAI Comput. Conf. (SAI)*, Jul. 2016, pp. 545_552.

[8] D. P. Yellamma, D. B. C. Narasimham, and M. T. Kumar, ``Cloud computingsecurity using secret sharing algorithm over singleto multi-clouds,"*Latest Res. Eng. Manag.*, vol. 1, pp. 1_6, Apr. 2016.

[9] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, ``Intelligent cryptographyapproach for secure distributed big data storage in cloud computing," *Inf.Sci.*, vol. 387, pp. 103_115, May 2017.

[10] B. S. Rawal, V. Vijayakumar, G. Manogaran, R. Varatharajan, andN. Chilamkurti, ``Secure disintegration protocol for privacy preservingcloud storage," *Wireless Pers. Commun.*, vol. 103, no. 2, pp. 1161_1177,Nov. 2018.

[11] O. Zibouh, A. Dalli, and H. Drissi, ``Cloud computing security through parallelizingfully homomorphic encryption applied to multi-cloud approach,"*J. Theor. Appl. Inf. Technol.*, vol. 87, no. 2, pp. 300_307, 2016.

[12] K. Subramanian and F. L. John, ``Secure and reliable unstructured datasharing in multi-cloud storage using the hybrid crypto system," *Int. J.Comput. Sci. Netw. Secur.*, vol. 17, no. 6, pp. 196_206, 2017.

[13] S. Bogos, J. Gaspoz, and S. Vaudenay, ``Cryptanalysis of a homomorphicencryption scheme," *Cryptogr. Commun.*, vol. 10, no. 1, pp. 27_39,Jan. 2018.

[14] B. Ul Islam Khan, A. M. Baba, R. F. Olanrewaju, S. A. Lone, andN. F. Zulkurnain, ``SSM: Secure-split-merge data distribution in cloud infrastructure," in *Proc. IEEE Conf. Open Syst. (ICOS)*, Aug. 2015,pp. 40_45.

[15]C.Priya and Dr.R.Latha,“TaaS: A Framework for Trust Management in Cloud Computing Environments” in International Journal of Science and Research, volume 5, issue 9, 1402-05, ISSN 2319-7064(Online), DOI: 10.21275/ART20161879, September 2016.

[16]G.Gayathri and Dr.R.Latha,“Implementing a Fault Tolerance Enabled Load Balancing Algorithm in the Cloud Computing Environment” in International Journal of Engineering Development and Research (IJEDR), volume 5, issue 1, 249-256, ISSN 2321-9939(Online), 2017.