Data Encryption In Cloud

Yogita Nehar[1], Mr. Vinod Azad[2]
[1, 2] Department of Computer Science
[1, 2] Truba college of engg. & tech. Indore (m.p.)

I. PROPOSED RAILFENCE TECHNIQUE

Cloud computing provides efficient storage setting to store and retrieve the cloud user's data. Ensuring data security is a vital role to cloud users as well as cloud providers. Proposed security service processes the data, and then data are submitted to the cloud storage. Data encryption is done by choosing Railfence security service algorithm by the user. The encryption key used for algorithm is receivedfroma CSP to the user.

Algorithm #1 shows the proposed Railfence security service algorithmin CSP1. It is a symmetric encryption algorithm. It uses four keys for encryption and the same keys are used for decryption. The given plain text characters are converted into ASCII values. A square matrix is formed based on the number of characters in the plaintext. Maximum size of the matrix is 25X25. The square matrix is divided into three matrices called upper (UMAT), diagonal (DMAT) and lower (UMAT) matrix. Apply the encryption to the matrices UMAT, DMAT and UMAT individually by using the keys K1, K2, K3respectively. Another square matrix is constructed with an encrypted value. Nowthe text is read column by column.Order of understanding the column is based on order of Key K4. Finally, the ASCII code values are converted intocharacter value.This value is ciphertext.

Algorithm #1: Railfence Security Service Algorithm

```
1. encryption_text(T)
2. start
3. Convert (T) into ASCII code
4. N= count (T)

// N- number of characters in T

//form the matrix for N character, maximum size of
matrix is 25X25, if N>625 than divide the T into 625
character blocks and form matrix for each block.
5. matc =N/625
6. if matc>0
fori=1 to matc
Divide the T into 625 blocks, N=n1, n2, n3…nn// n1, n2, n3
are each individual matrix
end loop
end if
7. for p=1 to matc
8. Based on the value of N, form a square matrix MAT
[MXM] > N,M=M
9. Apply T into the matrix from left to right
10. Divide the Matrix MAT into three matrices called
UMAT,DMAT,LMAT

//UMAT-Upper Matrix, DMAT-Diagonal Matrix,
LMAT-Lower Matrix
11. Read the Text T by UMAT(U), DMAT(D) and
LMAT(L)matrix

//U, D, L- text of upper, diagonal and lower matrix
respectively
// generate the random number for keys
12. Get three random integer number as KEYS K1, K2, K3
for each matrix.
13. Apply the key K1, K2, K3 for U, D, L to get first
encrypted data

// [U-K1, D-K2, L-K3]
14. Arrange the encrypted text into another matrixMAT1
[MXM]based on number character in the key K4
15. Read the matrix MAT1 column by column in order of
key K4
16. Resultant text from step 15 is converted to ASCII
character code(C)

//C-Cipher Text
17. end loop
18. end
```

Algorithm #2 is used for the generation of random integer number from CSP2. This algorithm generates a random value. CSP1 instructs CSP2 to generate three integers valued key for K1, K2 and K3 and one string key for k4. These four keys are forwarded to the cloud user directly by CSP2.

Algorithm #2: Random Number Generation

```
1. intrandom_num_gen()
2. start
// generation of random using random() class
```

```
3. ran=new random().nextInt(100)
4. return ran
5. end
```

The proposed Railfence security service algorithm is applied on the non-numeric type of data. Railfence ensures the confidentiality of cloud data. It can protect the data in cloud storage from insiders and outsiders attacks. The keyused for encryption is kept by the cloud user, so the cloud storage provider does not have any knowledge about the key because the key is not communicated to them. Cloud users do not have any work burden to encrypt the data with Railfence. The hacker (insider or outsider) may get the encrypted data stored in the cloud, but they could not get a clear understanding about the data. It increases the confidentiality of the data stored in the cloud storage.

II. SIMULATION RESULTS

The proposed Railfence technique and key generation is implemented in JAVA. Simulation is performed in the cloud environment (Amazon EC2). The cloud user machine connected to the cloud server has the configuration of Windows Operating System with core i3 Intel processor and 4GB RAM. The user data are encrypted before it is uploaded and decrypted when it is retrieved from the cloud. Thus, the encryption is done in the user machine connected to the cloud. Time taken for encryption and decryption is calculated in the user machine. Amazon Elastic Compute Cloud (EC2) server is used for cloud storage. Key generation and Railfence techniques are developed as web service and hosted in the Amazon server.The Amazon micro instance has the following configurationasMicrosoft windows server 2008 Base 32 bitoperating system, 2.5 GHz Intel xeon processor, 613 MB RAM, 30GB of EBS (Elastic Block Storage). The users upload the data via user interface. Once the data are submitted, then they are encrypted and uploaded to the Amazon micro instance server. Security levels of the existing and proposed techniques are computed in Amazon server. Security level is analysed by using a security analysis toolcalled Hackman. This tool analyses the security level of proposed and existing techniques. This tool is installed in Amazon server for analysing the security level of each technique. Hackman attacks the encrypted text in the Amazon server. It uses different attacks like dictionary attack, brute force attack, etc. to retrieve the original text. Map the plain text with retrieved text to find the percentage of original text retrieval. Based on percentage mapping, security level of the proposed technique is estimated. In the same way, existing cryptography techniques security level are calculated and compared with the proposed technique. Performance and security level of proposed Railfence technique is compared with existing encryption techniques. Time taken for encryption and decryption is shown in Table 1 and Table 2 respectively. Security levels of proposed and existing techniques are compared and shown in Table 3.Simulation is conducted for different sizes of data. For each size of data, time taken for encryption, decryption and security level are noted and evaluated with existing techniques. Performance of proposed technique is measured by the time taken to complete encryption and decryption process.

Table 1. Performance Comparison based on Encryption Time (Milliseconds)

Size	**Encryption Techniques**			
	DES	3DES	Blowfish	RailfanceDES
1 MB	502	618	397	282
2 MB	967	1078	602	468
3 MB	1302	1422	891	656
4 MB	1701	1847	1073	889
5 MB	2108	2236	1207	1102
10 MB	4282	4404	2421	2253
15 MB	6331	6597	3642	3388

Table 1 represents the time taken for encrypting the data using proposed Railfence and existing techniques like DES, 3DES and Blowfish.

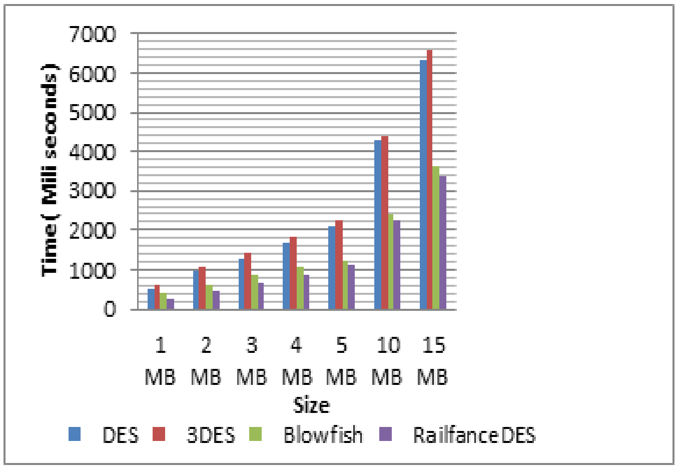
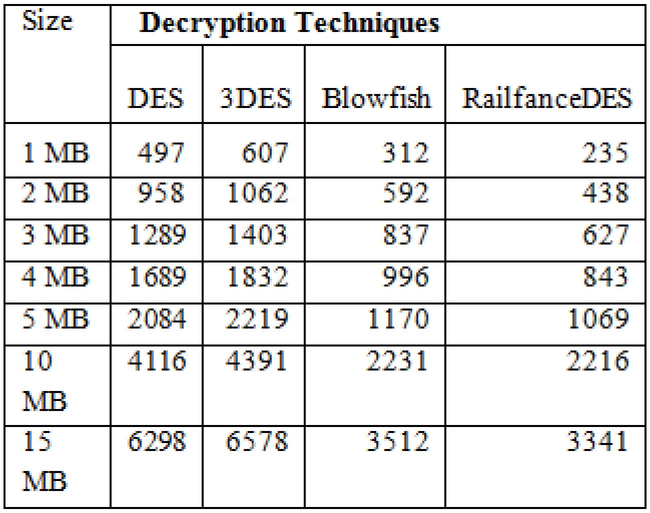


Figure 1. Performance Comparison based on Encryption Time

Table I and Figure 4 represent the performance comparison of proposed Railfence encryption algorithm with existing algorithms. The time taken by the existing and proposed encryption algorithms are calculated for different sizes of data. The result shows that the proposed Railfence algorithm has taken minimum time duration for encrypting the data of different sizes when compared to the existing algorithms.

TABLE II.PERFORMANCE COMPARISON BASED ON DECRYPTION TIME (MILLISECONDS)



Size	Decryption Techniques			
	DES	3DES	Blowfish	RailfanceDES
1 MB	497	607	312	235
2 MB	958	1062	592	438
3 MB	1289	1403	837	627
4 MB	1689	1832	996	843
5 MB	2084	2219	1170	1069
10 MB	4116	4391	2231	2216
15 MB	6298	6578	3512	3341

Decryption Time

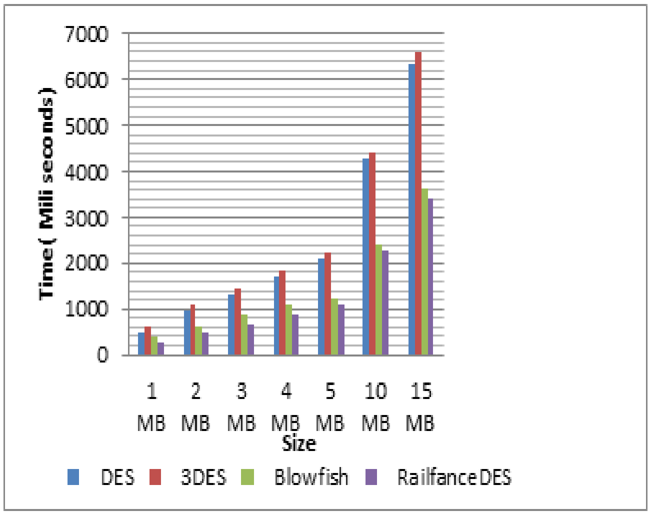


Figure 2 Performance Comparison based on Decryption Time

Table II and Figure 5 represent the performance comparison of decryption with existing techniques. The time taken by the existing and proposed decryption techniques are calculated for different sizes of data. The result shows that the proposed Railfence technique has taken minimum time duration for decrypting the data of different sizes when compared to the existing techniques

Table 2. COMPARISON OF SECURITY LEVEL

S.No	Techniques	Security Level(%)
1	DES	74
2	3DES	82
3	Blowfish	78
4	Railfence	89

Security Level

Table 3.

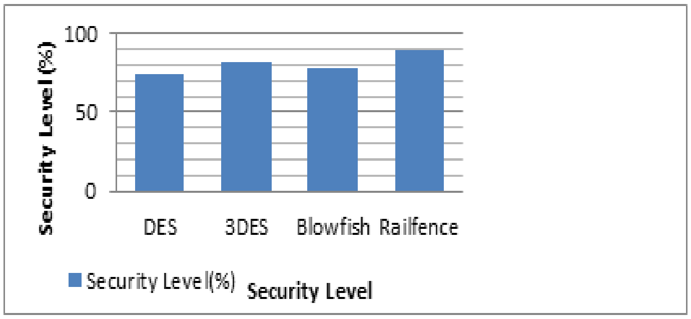


Figure 3. Comparison of Security Level

Table III and Figure 6 represent the comparison of security level based on the security analysis tool. The result shows that the proposed Railfence technique secures 89% of security that is higher than the existing techniques.

The above results show that the Railfence technique gives maximum security and better performance than existing techniques while storing the data in the cloud. Hence, the confidentially of the data stored in the cloud is achieved.

III. CONCLUSION

Cloud Storage is a cost-effective IT service to the general user or enterprise customer. Most of SMEs do not have the infrastructure to keep their data safe. Cloud storage provides plenty of storage capability with nominal cost. SMEs are interested in outsourcing their sensitive data to the cloud storage. However, there are some security problems with cloud storage.Due to this, enterprises are disinclined to use the cloud. Once the issues are resolved, cloud computing would be a trillion dollar business in the computing world. Data storage on un-trusted cloud creates data security as a challenging problem. The confidentiality parameter ensures data security in the cloud. This paper proposed a new cryptographic technique named Railfence to address the security problems in cloud storage. This Railfence technique is provided through SEaaS model. Encrypted data are stored on storage server while secret keys are retained by data owner and access to the user is granted by issuing the corresponding decryption keys. Railfence technique is based on a symmetric encryption technique. The data are encrypted before they are forwarded to the cloud storage. Hence, in this paper a new confidentiality technique has been proposed and implemented. Simulation results show the comparison of Railfence with existing techniques. From the results, it is observed that Railfence technique offers better performance and maximum protection to the data stored in the cloud than the existing encryption techniques.

REFERENCES

[1] I. Foster, Z. Yong, I. Raicu and L. Shiyong, (2008, 12-16 Nov. 2008), Cloud Computing and Grid Computing 360-Degree Compared, Paper presented at the Grid Computing Environments Workshop, 2008, GCE '08.

[2] NIST SP 800-145, "A NIST definition of cloud computing", [online] 2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf (Accessed: 23 December (2013).

[3] Gartner, "What you need to know about cloud computing security and compliance", (HeiserJ), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud-computing- Security (Accessed 23 December 2013).

[4] Z. Yandong and Z. Yongsheng, "Cloud computing and cloud security challenges in Information Technology in Medicine and Education (ITME)", 2012 International Symposium on, (2012), pp. 1084-1088.

[5] IBM, "what is cloud computing" [online] http://www.ibm.com/cloud-computing/in/en/what-is-cloud- computing.html (Accessed: 14 December 2013).

[6] IDG Cloud Computing Survey: "Security, Integration Challenge Growth", [online], http://www.forbes.com/sites/louiscolumbus/2013/08/13/idg-cloud-computing-survey-security-integration-challenge-growth.html/(Accessed: 28 December 2013).

[7] D. Catteddu and G. Hogben, "Cloud computing: Benefits, risks and recommendations for information security", European Network and Information Security Agency (ENISA), pp. 1–125.

[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, (2011), pp. 1-11.

[9] A. A. Soofi and M. I. K Fazal-e-Amin, "A Review on Data Security in Cloud Computing", International Journal of Computer Applications, vol. 94, no. 5, (2014), pp. 12-20.

[10] T. Dillon, C. Wu and E. Chang, "Cloud computing: issues and challenges", Paper presented at the Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. (2010).

[11] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain", Journal of Systems and Software, vol. 80, no. 4, (2007), pp. 571-583.

[12] A. K. M. Fazal-e-Amin and A. Oxley, "A review on aspect oriented implementation of software product lines components", Information Technology Journal, vol. 9, no. 6, (2010), pp. 1262-1269.

[13] A. K. M. Fazal-e-Amin and A. Oxley, "A Review of Software Component Reusability Assessment Approaches", Research Journal of Information Technology, vol. 3, no. 1, (2011), pp. 1-11.

[14] K. Hashizume, D. Rosado, E. Fernández-Medina and E. Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, vol. 4, no. 1, (2013), pp.1-13.

[15] R. Anane, S. Dhillon and B. Bordbar, "Stateless data concealment for distributed systems", Journal of Computer and System Sciences, vol. 74, no. 2, (2008), pp. 243-254.

[16] U. Somani, K. Lakhani and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing", Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on. (2010, 28-30 Oct. 2010).

[17] W. Cong, C. Ning, L. Jin, R. Kui and L. Wenjing, "Secure Ranked Keyword Search over Encrypted Cloud Data", Paper presented at the Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. (2010, 21-25 June 2010).

[18] H. Shuai and X. Jianchuan, "Ensuring data storage security through a novel third party auditor scheme in cloud computing", Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on. (2011, 15-17 Sept. 2011).

[19] Vamsee and Sriram, "Data Security in Cloud Computing," in Journal of Mathematics and computer sciences, vol. 2, no. 1, (2011), pp. 15- 23.

[20] S. K. Sood, "A combined approach to ensure data security in cloud computing", Journal of Network and Computer Applications, vol. 35, no. 6, (2012), pp. 1831-1838.

[21] E. M. Mohamed, H. S. Abdelkader and S. El-Etriby, “Enhanced data security model for cloud computing”, Paper presented at the Informatics and Systems (INFOS), 2012 8th International Conference on. (2012, 14-16 May 2012).

[22] J. Singh, B. Kumar and A. Khatri, “Improving stored data security in Cloud using Rc5 algorithm”, Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on. (2012, 6-8 Dec. 2012).

[23] Z. Lan, V. Varadharajan and M. Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage”, Information Forensics and Security, IEEE Transactions on, vol. 8, no. 12, (2013), pp. 1947-1960.

[24] J. Taeho, L. Xiang-Yang, W. Zhiguo and W. Meng, “Privacy preserving cloud data access with multi-authorities”, Paper presented at the INFOCOM, 2013 Proceedings IEEE, (2013, 14-19 April 2013).

[25] Y. Ching-Nung and L. Jia-Bin, “Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing”, Paper presented at the Biometrics and Security Technologies (ISBAST), 2013 Internationa Symposium on. (2013, 2-5 July 2013).

[26] P. Rewagad and Y. Pawar, “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. Paper presented at the Communication Systems and Network Technologies (CSNT), 2013 International Conference on. (2013, 6-8 April 2013).

[27] M. S. Abolghasemi, M. M. Sefidab and R. E. Atani, “Using location based encryption to improve the security of data access in cloud computing”, Paper presented at the Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on. (2013, 22-25 Aug. 2013).

[28] Kalpana and singaraju, “Data Security in Cloud Computing using RSA Algorithm,” in International Journal of Research in Computer and Communication technology (IJRCCT), vol. 1, no. 4, (2012).

[29] Q. Liu, G. Wang and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment”, Information Sciences, vol. 258, (2014), pp. 355-370.