Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 1, 2021, Pages. 5321 - 5329
Received 15 December 2020; Accepted 05 January 2021.

An Effective Secure Storage of Data in Cloud Using ISSE Encryption Technique

S Sindhura[1,*], S Phani Praveen[2], Shaik syedbi[3], V. Krishna Pratap[4], TBalaMurali Krishna[5]

[1,*]Assistant Professor,Department of Computer Science and Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, AP, India.

[2,]Assistant Professor, Department of Computer Science and Engineering, PVPSIT, Vijayawada,AP, India.

[3]Associate professor, Department of Computer Science and Engineering, Samarauniversity, Ethopia.

[4]Assistant Professor, Department of Computer Science and Engineering, NRIT, Guntur,AP, India.

[5]Professor, Department of Computer Science and Engineering, SSIET, Nuzvid, Andra Pradesh, India.

ssindhurapraveen@gmail.com[1],*, phani.0713@gmail.com[2], sfajju.syed@gmail.com[3], pratapv9@gmail.com[4],balu.thati9@gmail.com[5]

Abstract: Cloud computing is most widely used for managing the services within the web. Security is most widely seen in many applications. Especially in cloud computing data storage security plays the major role. Many security algorithms are proposed by the various authors that are worked based on encryption and decryption. Many issues are identified in terms of security such as data loss while data storing in the cloud storage. An integrated dynamic one time password security with strong key is generated to the document or file which can be stored in the cloud storage called as an integrated searchable symmetric encryption-2 (ISSE-2). For searching and symmetric encryption scheme triple DES algorithm is introduced in this paper. Encryption and decryption is most important in this system to provide security for the data.

Keywords: Cloud Computing, DES, ISSE-2, Encryption and Decryption.

1. Introduction

Every software companies are converting their data storages to cloud storage. Because of security and privacy cloud is most preferable for any of the organizations to maintain the secure data storage and can access the data from anywhere of the world. Cloud computing services will provide the on-demand response to the multiple users data that supports the multiple device and compatibility. Traditional storage servers are with very limited storage and provides very less security and privacy to the data stored in the cloud. From the service point of view cloud storage provides the efficient and dynamic facilities of the users storage data. In cloud, the data usage is as per the demand and pay as per the usage or requirement. This includes the SAAS, PAAS, IAAS etc. User can use wide range of available services and can pay only for utilized services.

In this paper, the proposed system focus on providing the security for the cloud storage by using DES algorithm that provides the security for data available in the cloud. Every file in this cloud will have the encryption key and decryption key. Three types of users are present in this scenario such as end user, cloud admin, data owner[22-25]. The data owner uploads and saves the data with public key generation and the entire data file is converted to the encryption. End user plays the major role in this system to access the required data from anywhere with the permission from cloud server and data owner[12][13]. If the end user wants any data file from the cloud, two requests are sent to the cloud server and data owner. Cloud server sends the encryption key to the end user and data owner sends the decryption key to the end user. Because of the security reasons the two keys concept is used. DES algorithm is most widely used algorithm which provides the strong security for the large data file sizes. The maximum data that can be stored in this file is 100 MB. To access the selected data storage key the one time password that sends to the authorized user mail. The organization of the paper as follows. In section 2 explains about the various securities, resource provisioning and other cloud features. Showing the comparative study on various methods with challenges. Section 3 and provides the brief description about the existing approaches and its dis-advantages and proposed methodology and introduces the Laplace transform for encryption and decryption of the data with steps. Section 4 explains about the experimental results with comparative analysis on existing systems. Conclusion and future scope is included in section 5 and 6 respectively.

2. Literature Survey

In this paper [1], the author proposed the hybrid encryption and decryption for the data storage in the cloud that provides the three encryption systems or approaches. The author explains about the three different types of round for the encryption and data process, and from the many number of securities can be provided for the cloud storage. In this first stage, the plain text is converted to the encrypted data by using the security algorithm on the selected data i,e data uploaded by the user. In the second stage, the the selected odd number letter is appended with the next letter after the odd position letter and then the data processing is performed on joining basis. The result of the second encryption takes three co-efficient utilized for the fourth stage of round encryption [17-21]. The output algorithm provides the

Received 15 December 2020; Accepted 05 January 2021.

efficient security for the data that provides the effective compressed data and file reduced to the 55% from the actual data.

In this paper [2] author present another procedure which uses BLS strategy for encryption which utilize a key matching framework and store the information with encrypted text, further transfer to the cloud worker server farm. This paper likewise uses the hashing procedure SHA-1 which is an honesty check strategy for the information beat for the respectability and adjustment change[3][14]. The security of this mark plot relies upon another issue, specifically k-CAA or k + 1EP. This plan permits a shorter mark plot than the FDH signature conspires. Likewise, creator utilizes BLS based plan for information security and capacity reason [15][16]. In this paper[4] they have worked with different quality classification, trustworthiness, accessibility, responsibility, and protection preservability and played out the different security concern issues in angles, creators have deliberately examined the security and security issues in distributed computing dependent on a property driven technique, We have recognized the most agent security/protection credits (e.g., secrecy, respectability, accessibility, responsibility, and protection preservability), just as talking about the weaknesses, which might be misused by foes so as to perform different assaults.

S.No	Name of the encryption technique	Citation	Challenges in existing system
1	Hybrid Encryption Scheme (HES)	Rashmi Singh et.al[1]	Focused on reducing the size of the data with compression algorithms which is uploaded in cloud.
2	Effective Multi-faceted Cost Model	Phani Praveen et al.[15]	Focused on reducing the cost but not security
3	An Algorithm for Rank Computing Resource Provisioning	Phani Praveen et al.[16]	Focused on resource allocation in cloud but not security

Table1 : Comparison of various challenges in Security issues of storage in cloud.

The author in this paper[5] mainly concentrates on the two round content-based encryption that uses the symmetric based key encryption technique for data prevention, this computation executes the twofold extension based computation, roundabout cycle moving activity is additionally shown with the key encryption process which is symmetric and it is used by the user. In this system, various algorithms such as ECC, RSA, and DES and also 3DES, Blowfish and AES. Researchers introduced a prototype whcih is used to works on critical analysis to work on various slandered identity protocols SAML,OIDC and OAuth. This also shows the analysis and how it works and usage[8][9]. Various advantages and dis-advantages are identified to increase the usage of various In conclusion; it discusses their standard identity protocol for all types (CC) models [6][10]. The author explains about the hybrid cryptosystem which is combination of Blowfish and RSA algorithm. This method or technique based on both symmetric and asymmetric cryptography [7][11].

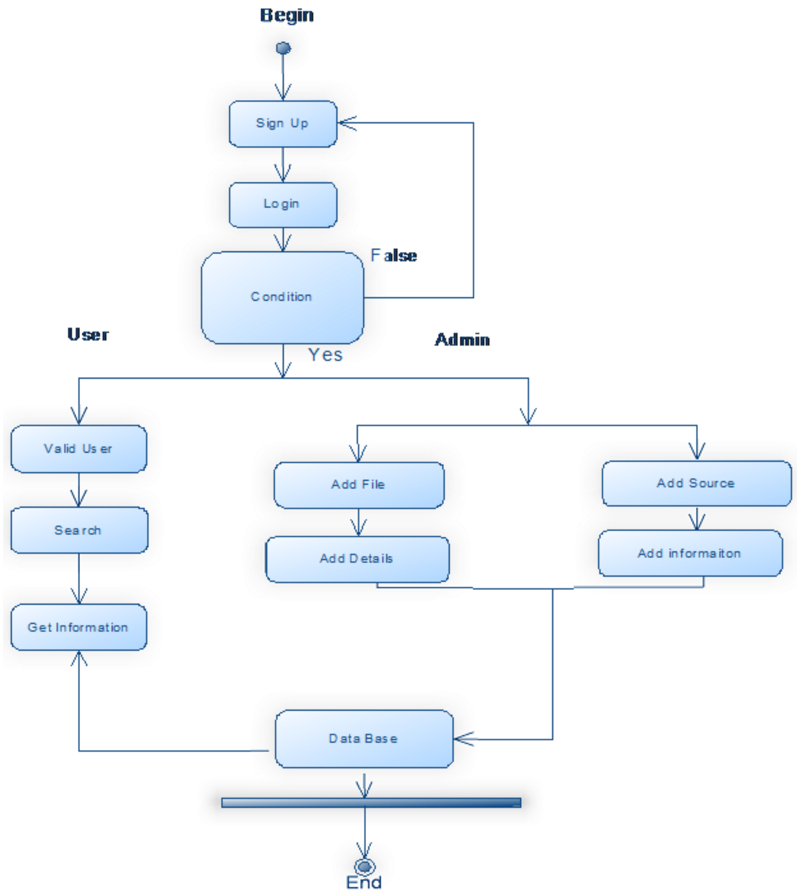

Figure1: Architecture of Proposed System

Identity Based Cryptography (IDCrypt)

In the existing system is called as IDcrypt, many security and privacy algorithms are provided to maintain the strong data storage with security algorithms. This system faces many challenges such as file size and time taking process to encrypt and decrypt. Many challenges are discussed in this but the multiple numbers of indexes and the encrypted data is shared between the multiple users[12]. To overcome the above issues the existing system introduced the IDcrypt is the system integrated with security algorithm with very limited features and functionalities. The searching process is called as token-adjustment search which gets the limited number of files based on the public-key encryption.

Dis-Advantages in IDCrypt:

- Lack of integrity and confidentiality

- Compatible for less data.

3. Proposed Methodology

For searching and symmetric encryption scheme triple DES algorithm is introduced in this paper. Encryption and decryption is most important in this system to provide security for the data. The following system is integrated with the proposed system.

An Integrated searchable symmetric encryption-2 (ISSE-2)

Data owner or admin: upload the file such as text files. The document is encrypted and key is generated save it in the cloud storage or database.User: The registered users search the data according to the requirement. After searching few files are extracted and if the user wants any file to download. The key should be given by the user. This is to be sent by the admin to the user after requesting by the user.The length of the every data present in this system provides the fixed number c. From the most of the data document set the keyword most widely used to get data. Before developing the index for the selected document, the most of the number of clount occurrence is present for the key. Another way of providing the security is setting the number c for the total number of documents. This method is more effective with fast creation of encryption and decryption. Simple Mail Transfer Protocol (SMTP) is the general protocol for utilizing email services with any programming language. SMTP provides the way to send and receive email messages. SMTP is the protocol which is used to integrate the mail programming to this system. This is used to send mails to the authorized users from the admin account. The Data Encryption Standard (DES) is used to provide security is many ways. This is the universal algorithm that provides the global security for the data which presents in anywhere.

Mathematical Equations for Encryption and decryption using Laplace Transform

1.The Laplace Transform: If *x (a)* is a function defined for all positive values of a, then the Laplace transform of *x (a)* is defined as

$$L(x\,(a)) = \int_0^\infty x\,(a)e^{-st}dt = F(s)$$

Provided the integral exists, where the parameter s is a real or complex number. We can also define inverse of laplace transform as

$$x\,(a) = F^{-1}(F(s))$$

Encryption Steps:

Step 1: a=(y, z) is the primary key.

Step 2: sample plain text t_0, t_1, t_2……t_{10}.

Received 15 December 2020; Accepted 05 January 2021.

Step 3: for the values of plain text the ASCII are A_0, A_1 ….A_k.

Step 4: Calculate $Bi = A_i q^i (y + i) fori = 0, 1, 2, \ldots k$

Step 5: Calculate Z_i and R_i with the given formula $B_i = (Q_i * n) + R_i sothatB_i = R_i modn, where\ 1 \leq R_i \leq n$

Step 6: sample plain text Q_0, Q_1, Q_2……Q_k is second key.

Step 7: C_i is the ASCII symbol belongs to R_i, i=0, 1,…, k.

Step 8: the result is Co, C1, C2, … Ck.

Decryption Steps:

Step 1: The symbol of R_i compatible to Ci, i=0, 1, …, k.

Step 2: Calculate $Bi = (Q_i * n) + R_i fori = 0, 1, 2, \ldots k$

Step 3: Calculate $M_i = \frac{B_i}{q^i \times (p+i)}, wherei = 0, 1, 2, \ldots k$

Step 4: $m_i = ASCIIvalueofM_i fori = 0, 1, 2, \ldots k$

Step 5: Output (decrypted message) $m_{0,} m_{1,} \ldots m_k$.

4. Evaluation Results

The implementation is done by using the java as programming language and NETBEANS 8.0.2 and JDK 1.8 and MYSQL as the database. In this paper, three users play the major role with creating the required encryption keys for hashing and encryption operations. The additional feature that we are providing is document search based on the keyword. If the user wants any document related to the topic they can search with the keyword. The data retrieved rapidly with huge number of results. If the user selected one file, the key should be entered by the user that the user received the file from data owner and cloud server. This key is received to the authorized users mail. For the searching of data user calculates and sends the trapdoor encryption of the queried keywords to the cloud to initiate a protocol to search for the requested keywords in the corpus.

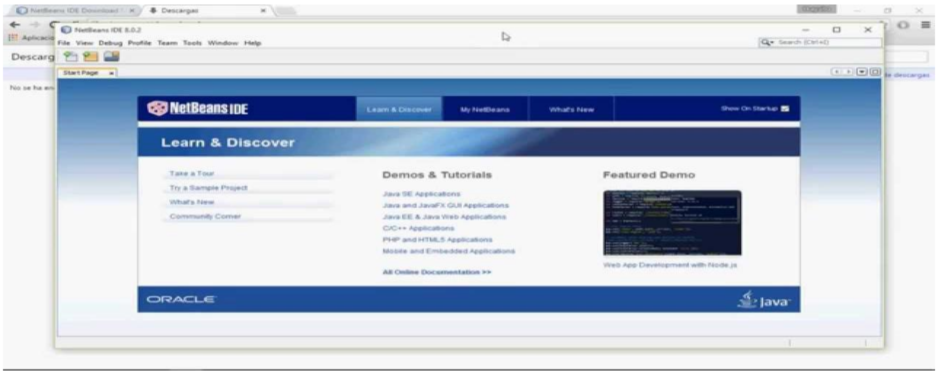

Figure 2: NetBeans 8.0.2 Software

Received 15 December 2020; Accepted 05 January 2021.

File Sixe (MB)	Time (sec)	
	Hybrid Encryption Scheme (HES)	ISSE-2
10 MB	33.43	12.32
20 MB	39.45	14.23
30 MB	40.54	15.43
40 MB	59.54	16.33

Table:2 shows the maximum file size with the proposed system ISSE-2

The total time taken for the data encryption is given below.

	File Size (Kb)	Time
Hybrid Encryption Scheme (HES)	20	0.99
ISSE-2	20	0.65

Table:3 Shows the performance of the proposed system

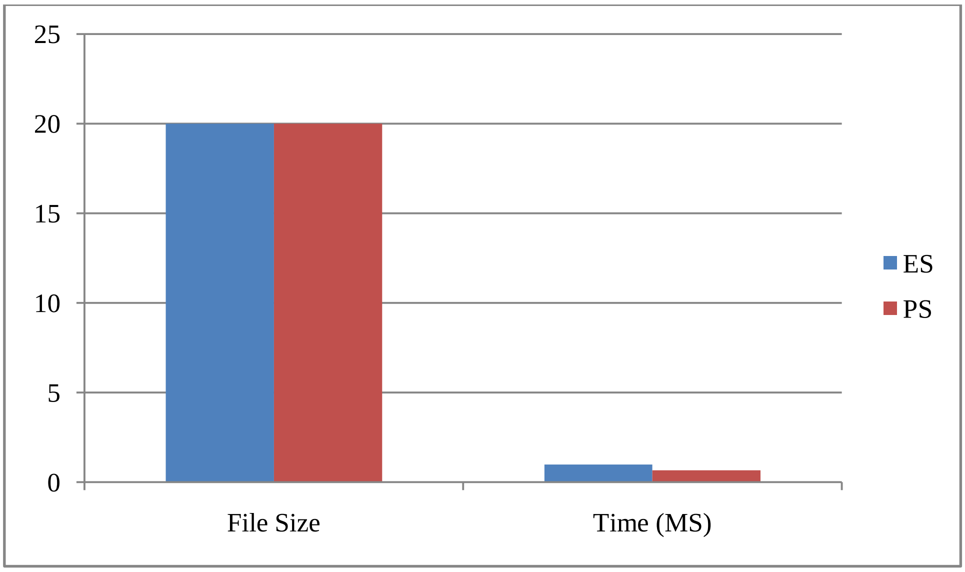

Figure: 3 Shows the performance of the existing system with previous references and proposed system with implemented with proposed system

5. Conclusion

Cloud computing is most emerging technology. In this paper, an advanced methodology is utilized called as integrated searchable symmetric encryption-2 (ISSE-2). ISSE-2 mainly focused on providing the security and privacy to the data which is stored in the cloud storage. SMTP is integrated to ISSE-2 to send the required encryption and decryption key to the authorized end-user. It is very important in this system to analyze the user status weather the user is authorized or not. Proposed methodology prevents the attacks that are done by the malicious users. Efficient and trusted security is integrated with the DES algorithm.

6. Future Scope

Cloud is developing very rapidly. Many challenges such as cost, security, computation and execution. In feature cloud computing integrates with Internet of thing (IoT) and Artificial Intelligence (AI). These technologies will give boost to the present cloud environment.

References

[1] RashmiSingha,IshaPanchbhaiyaa ,AbhishekPandeya& R H Goudar ,"Hybrid Encryption Scheme (HES): An Approach for Transmitting Secure Data over Internet", International Conference on Intelligent Computing, Communication & Convergence (ICCC2014),Elsevier.

[2] NanditaSengupta∗ and RamyaChinnasamy,"Contriving Hybrid DESCAST Algorithm for Cloud Security", Procedia Computer Science 54 (2015) 4756,Elsevier.

[3] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing,"http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.

[4] Zhifeng Xiao and Yang Xiao,– "Security and Privacy in Cloud Computing" IEEE June 2013 conference.

[5] SourabhChandraa*,BidishaMandalb , Sk. safikulAlamc , Siddhartha Bhattacharyya," Content based double encryption algorithm using symmetric key cryptography", Procedia Computer Science 57 (2015)1228 – 1234,Elsevier.

[6] Pachipala Yellamma1, P.Dileep Kumar, K.SaiPradeep Reddy, L.Sri Harsha, N Jagadeesh,"Probability of Data Leakage in Cloud Computing", International Journal of Advanced Science and Technology Vol. 29, No. 6, (2020), pp. 3444-3450, ISSN: 2005-4238 IJAST.

[7] Pachipala.Yellamma, P.S. S. Rajesh, V.V.S.M.Pradeep, Y.B.Manishankar," Privacy Preserving Biometric Authentication and Identification in Cloud Computing", International Journal of Advanced Science and Technology Vol. 29, No. 6, (2020), pp. 3087- 3096, ISSN: 2005-4238 IJAST.

[8] PachipalaYellamma," Advanced Q-MAC optimal Resource allocating for dynamic application in mobile cloud computing using Qos with cache memory, International Journal of Engineering & Technology, 7 (3.1) (2018),pp 143-146.

[9] Ramya, V. U., &Rao, K. T. (2018). Sentiment Analysis of Movie Review using Machine Learning Techniques. International Journal of Engineering & Technology, 7(2.7), 676-681.

[10] Deshmukh S., Aghav J., Rao K.T., Rao B.T. (2017) Avoiding Slow Running Nodes in Distributed Systems. In: Satapathy S., Bhateja V., Raju K., Janakiramaiah B. (eds) Computer Communication, Networking and Internet Security. Lecture Notes in Networks and Systems, vol 5. Springer, Singapore. https://doi.org/10.1007/978-981-10-3226-4_41

[11] Vadlamudi, D., Rao, K. T., Vidyullatha, P., &RajasekharReddy, B. (2018). Analysis on digital forensics challenges and anti-forensics techniques in cloud computing. International Journal of Engineering & Technology, 7(2.7), 1072-1075.

[12] Praveen, S. P., Rao, K. T., &Janakiramaiah, B. (2018). Effective allocation of resources and task scheduling in cloud environment using social group optimization.Arabian Journal for Science and Engineering, 43(8), 4265-4272.

[13] Phani Praveen, S., &Rao, K. T. (2018).Client-Awareness Resource Allotment and Job Scheduling in Heterogeneous Cloud by Using Social Group Optimization. International Journal of Natural Computing Research (IJNCR), 7(1), 15-31.

[14] Praveen, S. P., &Rao, K. T. (2018). An Optimized Rendering Solution for Ranking Heterogeneous VM Instances.In Intelligent Engineering Informatics (pp. 159-167).Springer, Singapore.

[15] N.Krishnaraj,M.G.Kavitha,T.Jayasankar,K.Vinoth Kumar, “A Glove based approach to recognize Indian Sign Languages”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6, March 2019, pp.1419-1425.

[16] Praveen, S. P., &Rao, K. T. (2019). An Effective Multi-faceted Cost Model for Auto-scaling of Servers in Cloud. In Smart Intelligent Computing and Applications (pp. 591-601). Springer, Singapore.

[17] Praveen, S. P., &Rao, K. T. (2016). An Algorithm for Rank Computing Resource Provisioning in Cloud Computing. International Journal of Computer Science and Information Security (IJCSIS), 14(9).

[18] Praveen, S. P., Tulasi, U., &Teja, K. A. K. (2014). A cost efficient resource provisioning approach using virtual machine placement. Int. J. Comput. Sci. Inf. Technol., 5(2), 2365-2368.

[19] R.ArunPrakash, T.Jayasankar, K.VinothKumar, “Biometric Encoding and Biometric Authentication (BEBA) Protocol for Secure Cloud in M-Commerce Environment”, Appl. Math. Inf. Sci. Vol.12, No.1, Jan 2018, pp.255–263.
DOI: http://dx.doi.org/10.18576/amis/12012

[20] G.Mani, V.Nivedhitha, N.S.Pradeep, T.Jayasankar and K.Vinothkumar , “Reliable Wormhole Detection System (RWDS) Based Secure Routing and Authentication for Environmental Monitoring”, Journal of Green Engineering (JGE) Vol.10, No.3, pp.734-749,March 2020

[21] Priyanka Parvathy, D Kamalraj Subramaniam, G.K.D PrasannaVenkatesan, P. Karthikaikumar , Justin Varghese, T.Jayasankar, “Development of Hand Gesture Recognition System Using Machine Learning”, Journal of Ambient Intelligence and Humanized Computing (2020). https://doi.org/10.1007/s12652-020-02314-2.

[22] Praveen, S. P., &Tulasi, U. (2013). A Study on Qos Challenges in Cloud Computing. IJCC, 2(1).

[23] N. Krishnaraj, P. Ezhilarasu, X Z Gao “Hybrid Soft Computing Approach for Prediction of Cancer in Colon Using Microarray Gene Data” , Current Signal Transduction Therapy Vol.11 (2),pp71-75,June 2016.

[24] M.Anuradha, T.Jayasankar, PrakashN.B, Mohamed Yacin Sikkandar, G.R.Hemalakshmi, C.Bharatiraja,A. Sagai Francis Britto, “IoT enabled Cancer Prediction System to Enhance the Authentication and Security using Cloud Computing,” Microprocessor and Microsystems (Elsevier 2021), vol 80, February, (2021) https://doi.org/10.1016/j.micpro.2020.103301

[25] T.Jayasankar, R.M.Bhavadharini, N.R.Nagarajan, G.Mani, S. Ramesh, Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform”, European Journal of Molecular & Clinical Medicine (2021), Volume 08, Issue 01, 2021,pp.1075-1089