International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Multiple key Generation for Securing Data Sharing and Backup

Hariharan.R, Jayashree.D, Vishal Chauhan, Vibek Jyoti Roy, Anandhi K

Abstract: ***Currently a data sharing and data backup is been maintained by the intermediator of cloud admin provider also to reduce the cost of intermediator management and to get an authentication. It is introducing to provide a security and efficient access to large amount of outsourced data. In this project we are proposing a key distribution to solve the problem (encryption and decryption). As the user is provided two types of key by the admin to secure the data outsourcing and data backup which is been encrypted and decrypted so that threading and attacks can be reduced using cryptography based key mechanism. We are introducing a key mechanism using RSA and AES for generating keys files to secure the data. By this cryptographic key mechanism, the cloud users are free from the data management, consumption of time, cost.***

Index Terms: Data security, RSA (key mechanism), AES (encryption, decryption), cloud computing

I. INTRODUCTION

The Cloud computing is the demand accessibility of computer capitals especially data of client and computing short of any direct dynamic management [2]by the user the main characteristics of cloud services in which you pay for service before you use it and in a web based service this model is usually connected with a software as a service provider. Cloud computing runs a suitable way of opening computing services in independent of the hardware we use or any physical location it releases the need for storing information on your computer or mobile device or gadget with the statement that any information might[3] be exposed with fast period and certainly accessed through internet. Cloud computing offers customers with a virtual computing arrangement. Which enables them to store the data and run the presentations. In addition, the Cloud computing presents new security challenges as client cannot fully trust from cloud providers. Cryptography mechanism in cloud computing used to secure the data in cloud computing architecture with the algorithms and this computing model, which is ambitious by markets of scale and is been distributed on large-scale software, system and platform, and virtualization components. Whereas the IT services similar to on-demand
services is accessible by authorized member at anytime and anywhere. In addition, the cloud offers an infinite storage Space capacity for the user to store their data and provides the way for data backup by hash algorithm so that the user can retrieve the data at any time using cloud service. They can use the google drive, drop box to store the data. As per in the proposed work two security key distribution with public and private is been provided by the cryptographic mechanism from the cloud admin to the users.
These [8]cryptographic mechanism will provide security when the user upload or download data from the distribution to provide the security for that first the user must need to ensure their own personal details to register in an authorized party in cloud server. After the registration and choosing the group the cloud admin will give the keys to secure the data, which is, proposed by using a key mechanism of RSA and AES algorithm to secure the data. The problem of storing data is it can data are likely to be misused by the cloud provider or non-member of the group so we proposed this cryptographic mechanism for the client's data security

II.LITERATURE SURVEY

[1] Cloud-computing is the long-term dream of computing as an effectiveness, which is been possible to convert a big part of an IT sector. It makes the software even smarter as a service. In modelling way IT hardware is deliberate and it is been purchased the developers are with new concepts expose for new Internet services no longer require the large amount of costs in hardware to deploy their service or the human expense to operate it. The goal for this article is to reduce which to stop the misperception by helpful positions by giving simple records to measure evaluations with the cloud in technical and non-technical difficulties of cloud computing benefit. [4] The vital role of a cryptographic is to provide safety to secure the files by the authorized person in the group and it is been accessed by algorithm and access policy to secure the files, which is uploaded and downloaded. In an overview for the advantage of a cryptographic mechanism, we design an official requirement so that only the authorized person and cloud admin takes the responsibility in controlling and secure the files we define in more aspect the appropriate cryptographic method including encryption with evidence of storage and value based encryption.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Hariharan.R,* Department of Information Technology ,Veltech Rangarajan Dr.Sagunthala R&D institute of science and technology, Chennai,India.
Jayashree.D, Department of Information Technology ,Veltech Rangarajan Dr.Sagunthala R&D institute of science and technology, Chennai,India.
Vishal Chauhan , Department of Information Technology ,Veltech Rangarajan Dr.Sagunthala R&D institute of science and technology, Chennai,India.
Vibek Jyoti Roy, Department of Information Technology , VelTech Rangarajan Dr Sagunthala R&D Institute of Science and Technology, Avadi ,Chennai, India.
Anandhi K, Department of CSE,VelTech HighTech Rangarajan Dr Sakunthala Engineering College, Avadi ,Chennai, India

[5]Finally, with reference some cloud services we found that to secure the clients data to be secured with the cryptographic storage service.

[6] About the past half-century there is a huge expansion growth with an Information and Communications Technology (ICT). This computing process will come one day be the most valuable thing like water, electricity, gas, and telephone.

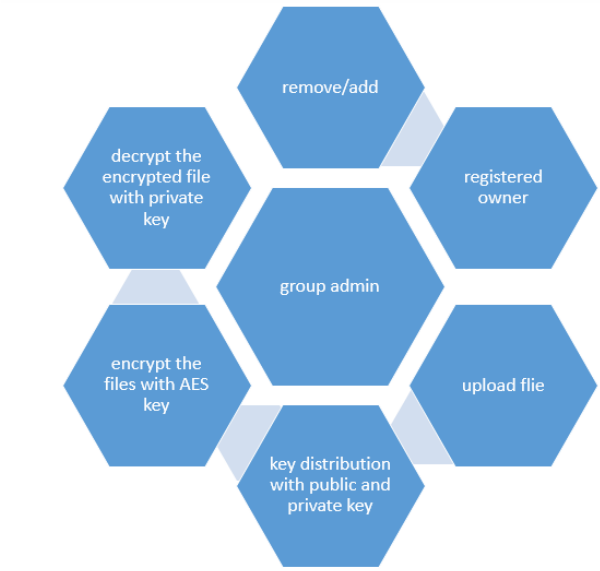

Fig1 : Proposed model

This following four standing services will afford a computing service with basic level which is deliberated[8] a vital as an intermediator in our humans daily life and many proposal have met to deliver this idea out of all this current trending proposal is used is known as cloud computing. [7]Generating Clouds with the business related resource allocation by using multi-tasking technologies such as Virtual Machines (VMs). Similarly there is an understanding between business-related resource management which include both client service management and computational risk management to withstand the Service Level Agreement oriented resource distribution and it expose the primary view by crossing the Cloud for energetically creating a wide cloud connections to contemporaneous some typical Cloud platforms.

III . PROPOSED WORK:

In our proposal work Fig 1 we introduce a concept that the data sharing[11] in cloud environment an also the securing the data's from the attacker, Cost. Here we are introducing this protection from the cryptographic key distribution by the group admin so the files will be encrypted and decrypted and the key's will be used according the accessing the authorized parties. By this process the data is secured reduce of cost and we can upload or download the data from anywhere, anytime. For this key cryptography or key mechanism, we have some process before the key distribution. First we should register own profile and after registering they must choose one group among the four group for login to upload/download. After choosing the group and details of the user must be, send to the admin after the admin acceptation only the use can login from the group. After the acceptation of request from the admin, the user can login the amount and can upload the file and while the process of uploading the files it will encrypt and decrypt and there will be a key distributions occurred to secure the file. Each files which the users uploading is been maintained by the admin and the encrypted files will be secured with the private key. The encrypted files will be decrypted with intelligence and will be posted in admins page if any second user's request to view the file it will been showed in admin page. If the second user wants to view the file, he is supposed to send a request to group admin because the group admin can encrypt and decrypt the files, which is been uploaded. To accept the request, the admin, check whether he is an authorized person in a group member then he accept the request to view the file in the admins page with the time duration of 30mins.The user can view or download it within then time duration of 30mins.If the user needs to download the file within the 30mins, the private key is provided by the admin. This process of proposed system is been enhanced by these techniques for getting a multiple key mechanism in cryptography.

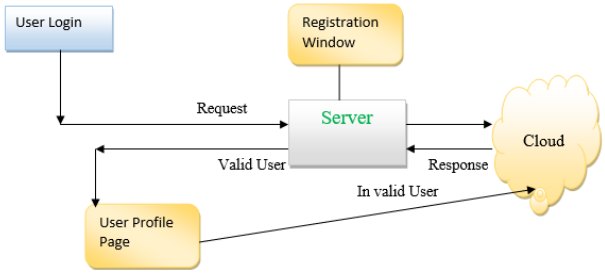

Fig 2: User Interface Design

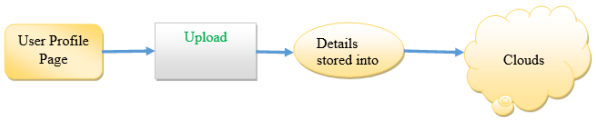

Fig 3: Generation of key and encrypting files

AES ALGORITHM:

The most popular and widely adopted asymmetric encryption algorithm likely to an encountered nowadays is the AES algorithm. ASE[9] algorithm is to encrypt and decrypt the data, which is upload by the user. The user's personal or important data will decrypt from the encrypted files so that only authorized parties can access it and those who are not an authorized cannot. Here the admin or user can only decrypt the data because decryption requires a secret key or password so that it could accessed again by authorized user. AES algorithm is six times faster than the triple DES. The DES (Data Encryption Standard) it is a mutual standard for data encryption and a form of secret key cryptography (SKC) which is been used only for encryption and decryption. Encryption key is been published for anyone to use and encrypt messages by public key and the process of plain text to cipher text. The reverse process of encryption from cipher text to plaintext is called decryption. This is been processed after the encryption for decrypt the file by private key with the intelligence.

RSA ALGORITHM:

RSA [10]algorithm is the process of algorithm, which is used, in asymmetric algorithm this means the connecting of two sides we use here for two form of key mechanism 1. Private Key ,2. Public key.

Private Key:

It is a key which is used for secure a private files and information.

Public key:

Public key is given to everyone and group users can use by the acceptation of group admin.

By this following procedure and the cryptographic mechanism, we made the following to secure data sharing, confidentiality and authentication in the cloud-computing environment.

The data owner to project the data from inside attacker carries out data sharing and Data backups in cloud. Unauthorized person data is stored in a form of AES algorithm the file to protect by public key and private key distribution so the data upload/download is been secured in this cryptographic key mechanism operation.

KDM:

Key Distribution Manager (KDM) is acted by the group admin distributes the public key and private key to the registered member in the group and the keys will be according to the encryption and decryption. Fig 2.

Data owner:

The encrypted data will be uploading a file in the cloud by the user from the group with the help of KDM, which is associated with the file along with API (access policy). API is accessed to use only by the authorized member from the group.

User registration:

Every user when they wants to upload their data in the cloud have to register before login first they are asked to choose the group among the 4 group then their personal details are being registered then the group admin accepts the request and sent a group id to login their personal id to upload the file.

Key generation:

RSA algorithm has used to produce a key mechanism fig 3. Private Key & Public key

Encryption:

Encryption is used to encrypt the files with public key to view for public users.

Decryption:

Decryption the user's data for secure from the attackers using private key and by using access policy and it is the reverse of encryption it is decrypt with intelligence with private key

IV. RESULT:

After the process of registration in the cloud group the testing is been processed with RSA and AES algorithm to secure the cryptographic server's data's in the cloud first the data has been encrypted to generate multiple keys of private and public key with time generation. Then the proposed work has been generated to secure the sharing data by inside attackers. Testing includes the test case which authenticate the interior process. Which validates the input and channelize the output. The code flow should be validated and the individual software units are tested. This test provides regular protests that function tested and made present as quantified by the technical specification documentation support and user manual. Functional testing is based on following things, this test verifies for the entire integrated software system requirements and also the orientation configuration. Which is based on the output time constraints and time taken for the process operation's response to the user requisite. This software testing is increasing integration testing with two or more integrated software running on single platform.

Build the test plan :

Projects contains various units which can be added for detailed processing. The testing strategy for each unit is done for bug testing in respective units. So that each units bugs can be identified and corrected swiftly.

V.CONCLUSION

As we discussed a secure sharing of data using RSA and AES algorithm to keep up the cloud server security. The KDM is used for all Key generation and distribution procedure in our proposed system. The performance is evaluated and the interference are attained on RSA key generation and AES encryption process by public and private key generation. By the interference our proposed system will be compatible for sharing data in cloud. We maintain policy based access mechanism to ensure authentication in cloud. In further advancements we can use multiple KDM to maintain the data with various access policies to prohibit insider threaten.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Kaminski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing." Comm. ACM, vol. 53, no.4, pp. 50-58, Apr. 2010.https://doi.org/10.1145/1721654.1721672
2. R. Hariharan *, C. Mahesh , P. Prasenna , R. Vinoth Kumar "Enhancing Privacy Preservation in Data Mining using Cluster based Greedy Method in Hierarchical Approach"Volume 9, Issue 3, January 2016 pp. DOI: 10.17485/ijst/2016/v9i3/86386
3. Dhilsath Fathima. M; Samuel, S. Justin "**Analysis of Machine Learning Algorithms for Effective Prediction of Cardiovascular Disease**" Journal of Computational and Theoretical Nanoscience, Volume 15, Numbers 9-10, September 2018, pp. 2920-2924(5).
4. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, 2010.https://doi.org/10.1007/978-3-642-14992-4_13
5. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010. https://doi.org/10.1109/infcom.2010.5462173
6. W. Wang, Z. Li, R. Owens, and B.Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Workshop Cloud Computing Security (CCSW), Nov.2009. https://doi.org/10.1145/1655008.1655016
7. A. Yun, C. Shi, and Y. Kim, "On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage," Proc. ACM Workshop Cloud Computing Security (CCSW), Nov. 2009. https://doi.org/10.1145/1655008.1655017
8. R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978. https://doi.org/10.1145/359340.359342
9. Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

10. Yellamma, P. , Narasimham, C. , and Sreenivas, V. , " Data security in cloud using RSA ", Proceedings of 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 4-6 July 2013.
11. R. Hariharan∗, S. Saran Raj and R. Vimala "A Novel Approach for Privacy Preservation in Bigdata Using Data Perturbation in Nested Clustering in Apache Spark" Journal of Computational and Theoretical Nanoscience, Volume 15, Numbers 9-10, September 2018, pp. 2954-2959(6),DOI: https://doi.org/10.1166/jctn.2018.7573.

AUTHORS PROFILE

Mr.R.Hariharan working as Assistant professor in Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology with 5 years of experience. He is a member in IEEE and CSI. .His research area is image processing and deep learning. He has published 15 article in various international journal and conference. Email_id:hharanbtech@gmail.com.

Ms.JAYASHREE.D is doing final year B.tech(IT) Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, her area of interest is Cloud computing and Security.

Mr.VISHAL CHAUHAN is doing bachelor of technology in Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, his area of interest is image processing signal processing , Deep learning. He has completed special training program in Deep learning in Asia university, Taiwan. He presented a paper in national conference.

Mr.VIBEK JYOTI ROY is doing bachelor of technology in Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, his area of interest is image processing and green computing. He has published 3 papers in various international journal and conference.

Ms.K.Anadhi working as assistant professor in VelTech HighTech Rangarajan Dr Sakunthala Engineering College. She published 3 articles in various international journal and conference. Her research area is image processing and deep learning.