International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 16385-16392

http://www.ripublication.com

Usage of Key-Aggregate Crypto With Steganography For Secured Data Sharing In Cloud Computing

S.Vinod Kumar[1], M.K.V Sreeram[2], Ms.S.Sarika.M.E. (PH.D)[3]

[1.] *UG student, Dept. of Computer Science, Sathyabama University, Chennai, India*

[2.] *UG student, Dept. of Computer Science, Sathyabama University, Chennai, India*

[3.] *Assistant Professor, Faculty of computing, Sathyabama University, Chennai, India*

Abstract

In this paper, we show how effectively the encrypted data are disclosed. When data owner stores the data in the cloud, before that the data is encrypted using AES (Advance Encryption Standards) algorithm. And so the encrypted information is covered in images using steganography technique. The image is hashed using Merkle's hash tree algorithm. Then the hashed values are stored in the cloud. When information is saved in the cloud, it produces the ADK (Aggregate Decryption key) key generation link it is mailed to the owner through email, the owner can authenticate it with his secret key and public-key, and then it produces the ADK key. That key is communicated to the user whenever the user asks for the access to the file. Then the TPA (Third Party Audit) checks the data whether the information is tainted or not using the Merkle's hash tree algorithm.

Keywords: Encryption, AES, STEGANOGRAPHY, ADk, Merkle's, TPA, Decryption

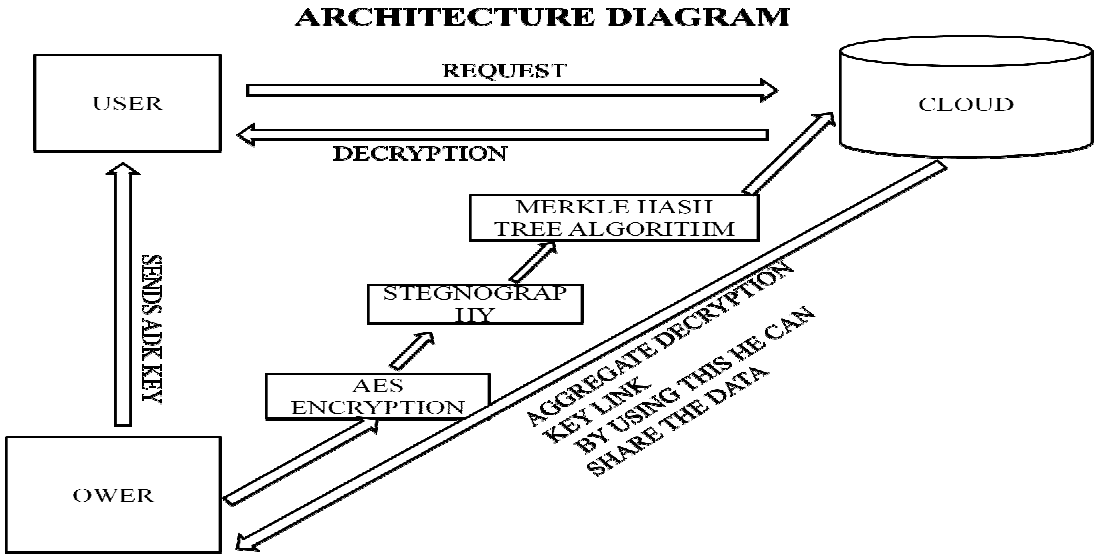
Introduction

Cloud: You can access your data where ever we want it. It provides services like software, platform, infrastructure (Saas, Pass,Iass). There are several organizations that provide cloud for free and paid service. Now a day's everyone who has the smart

phone or using the cloud, service Provider Company is Google, Yahoo, Apple, and Amazon etc. The problem with the cloud is lack of security since anyone can access the data anywhere Cloud storage is attracted lot people recently. In the project settings, we decide the income increase in the order of information outsourcing, which dishes up on the planned management of company information. It is equally well used as a center technology at the back a lot of online services for private applications.

To depend on the server, it is implemented to organize after authentication [2]. In a common tenancycloud computing environment, matters become even worse. Information from different networks will be located VM (virtual machine) but exist is on a single physical machine. Information is a goal VM could be stolen by instantiating one more VM Co resident with the target one [3]. About accessibility of files, there are a sequence of cryptographic systems which run as far as a third party listener to decide the accessibility of files on behalf of holder without releasing anything about the information [4], or trade off the data managers mystery [5]. Correspondingly, cloud clients, won't have the solid conviction that the cloud server performing a home business regarding security. A cryptographic arrangement, for instance, [6], which checks the security depended on number of theoretic suppositions are more alluring, at whatever point the client is not totally content with unquestioning the security of the VM or the earnestness of the mechanical stuff. These clients are invited to encode their data with their own particular keys before transferring them to the server. The primary issue is the means by which adequately the information is encoded, clients can download the scrambled information from the capacity then send them to others for imparting it, and however, it loses the estimation of distributed storage. Clients ought to have the capacity to delegate the right to gain entrance privileges of the imparting information to others so they can get to this information to from the server straightforwardly. In any case, discovering a skilled and secure approach to imparting incomplete information in distributed storage is not a little. Drop box taken as a sample that one keeps all private photographs in drop box, and that photograph ought, not to be seen by an alternate by method for hacking. That one can't feel to others on the security assurance instruments gave by Drop box, so she encodes all the photographs utilizing their own keys before transferring. One day, his companion’s requests to impart the photographs assumed control over all these years which her companions showed up in. He/she can utilize the offer anyhow the issue now is the means by which to delegate the decoding rights for these photographs to their companions. A conceivable alternative that he/she can send the key security. Commonly, there are two compelling routes for her under the customary encryption standard that encodes all records with a solitary encryption key and provides for her the relating mystery key straightforwardly. He/she encodes documents with different keys and sends to their companions, the relating Mystery keys. Clearly, the first strategy is deficient for all UN picked information may be likewise spilled to all others. For the second system, there are commonsense concerns on proficiency. The quantity of such keys is as much as the quantity of the imported photographs says, a thousand. Exchanging these mystery keys intrinsically obliges a safe channel, and putting away these keys obliges rather extravagant secure stockpiling. The expenses and complexities included for the most part increment with

the quantity of the decoding keys to be imparted. To put it plainly, it is overwhelming and expensive to do that. Encryption keys likewise come in two flavors-symmetric key or uneven (open) key. Utilizing symmetric encryption, When he/she needs the information to be begun from an outsider she needs to give encode or her mystery key; obviously, this is not generally attractive. By complexity, the encryption key and decoding key are diverse in broad daylight key Encryption. The utilization of open key encryption gives more adaptability for our applications. For instance, in big business settings each worker can transfer scrambled information on the distributed storage server without the learning of the organization's expert mystery key. In this way, the best answer for the above issue is that he/she scrambles documents with unique open keys, however just sends their companions a solitary (consistent size unscrambling key. Since the unscrambling key ought to be sent through a safe channel and kept mystery, little key size is constantly alluring. Case in point, we can't expect vast capacity for decoding keys in the asset compelled gadgets like PDAs, keen cards, or remote sensor hubs particularly; these mystery keys are generally put away in the sealed memory, which is moderately costly. The present examination endeavors for the most part centering on minimizing the correspondence necessities, (for example, data transfer capacity, rounds of correspondence) like total mark. On the other hand, very little has been carried out about the key module itself.



Proposed Work

Cloud servers:

Cloud servers are constructed with the files and the index information, are maintained in the main cloud server. The data are included in each cloud servers, and network construction is made with the entire data index present in each cloud server. The query is given to the highest cloud server, so that the main cloud server will verify the index information presented in it's & divert the query to the corresponding cloud servers.

Data User / Owner Registration:

Used to create a user application in which the user is permitted to access the data from the server of the cloud Service Provider. Here first the user wants to create an account and then only they are permitted to access the Network. Once the user sets up an account, they are to login into their account and request the Job from the cloud Service Provider. Based on the User's request, the cloud Service Provider will process the user requested Job and respond to them. All the user details will be stored in the database of the cloud Service Provider. In this project, we will design the User Interface. Frame to communicate with the cloud server by sending the request to the cloud server provider. The user can access the requested data if they authenticated by the cloud Service Provider.

Data Upload with Index Management

Data owner uploading the file encrypts with AES algorithm and public key. The index value means every file has to be searched by using an index value while uploading the cloud. Owner has to enter limited index values for every file using the shared public key. While uploading the file the cloud gives index value and a public-key. This index value, public key and files are encrypted with the AES algorithm and stored in the cloud server.Any accss to the file uploaded, a link will be sent to the cloud owner through an e-mail

AES

AES embodies three square figures. Each one figure encodes and decodes information in bitsutilizing cryptographic keys of separately. (Rijndael was intended to handle extra piece sizes and key lengths; however the usefulness was not embraced in AES.) Symmetric or riddle key figures utilize the same key for scrambling and unscrambling, so both the sender and the beneficiary must know how to utilize the same mystery key. All key lengths are regarded sufficient to secure portrayed data up to the "Mystery" level with "Top Secret" data obliging key lengths. Around exemplifies several making consideration of strides that combine substitution,

transposition and blending of the information plaintext and changes it into the last yield of cipher text.

As in figure, AES has demonstrated robust. The main fruitful assaults against it have been side-channel assaults on shortcomings found in the use or key administration of specific AES-based encryption items. (Side-channel assaults don't utilize beast power or hypothetical shortcomings to break a figure, yet rather adventure defects in the way it has been actualized.) The BEAST program misuse against the TLS v1.0 convention is a decent sample. TLS can utilize AES to scramble information, yet because of the data that TLS uncovered, aggressors figured out how to foresee the in statement vector piece utilized towards the being of the encryption process.

Different analysts have distributed assaults against diminished round adaptations of the Advanced Encryption Standard(AES), and the paper distributed in 2011 showed that utilizing a procedure called a biclique assault could recuperate AES keys quicker than an animal power assault by a variable of somewhere around three and five, contingent upon the figure variant. Indeed this assault, however, does not debilitate viable utilization of AES because of its high computational intricacy.

Steganography:

Steganography is the art or a practice of concealing a message within another image. Generally, the hidden messages will appear to be something else: images, articles, shopping lists, or some other cover text. In this module, we encrypt the files, index value using the shared public-key. The encrypted data are hidden in the image after which it will be saved in the cloud server.

ADK Generation:

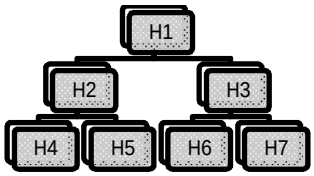
The ADK (aggregate decryption key) key will be generated whenever the file is uploaded The key is generated after validating the cloud owner by giving the master key. Every cloud owner has a master key during the registration in the cloud. Utilizing the master key the cloud owner generates the ADK key for every uploaded file.

User Authentication & Data Sharing:

The user will search the files but they cannot see the content. They need to get permission from the cloud owner even though the cloud user has a username, password and public key. They have to get the permission from the owner. The cloud owner will receive the user request and send the ADK key to the cloud user .The email sent to the cloud user has to be entered to view the files.

Merkle's Hash Tree Algorithm:

A Merkle's Hash Tree is a decently contemplated structure utilized for verification reasons, which is proposed to demonstrate productively that a set of components are unaltered and undamaged. It is used for diminishing the server recovery time. It is exercised by cryptographic techniques to verify the document squares. The tree is built as a paired tree where the leaf hubs are the hashes of the factual information values. The thought utilized as a part of this is to split the document up into various little pieces, apply hash to these pieces and consolidate iteratively and go over the ensuing hashes in a tree-like design with a solitary 'root hash'. The MHT (merkle's hash tree) is established by the customer and is put away at both the client and the server side.

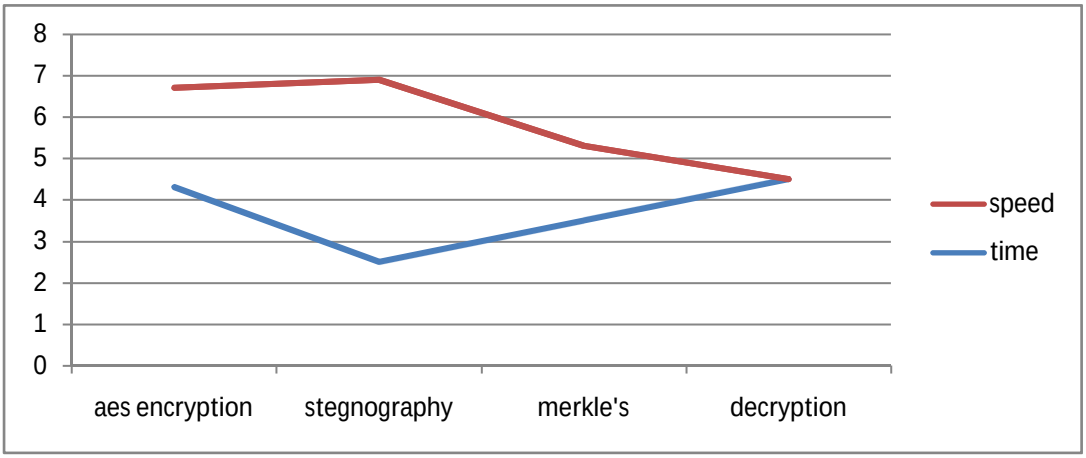


Data Integrity

Top Hash Code is placed on the TPA (third party audit) for verifying the integrity of the data. TPA will verify the data on a random basis by setting the corresponding encrypted part like The E1 to land up with H1. TPA will send a request to cloud server to provide H2. TPA will combine and form H12 and send request for H34. TPA will form H1234. Finally TPA will require for H5678 and combines to H12345678 which is the top hash code. This value is verified with the maximum hash code, which was provided by the Data Owner. By this way data integrity is achieved. If any unauthorized change in the data then automatic E mail alert is passed to the Data Owner

Performance Evaluation

Encryption and Decryption Time Figure below graphically speak to the time needed for encryption and unscrambling separately on distinctive document sizes. Conduct of charts demonstrates that for record size up to 1000 KB, when the file size is huge



Related Work

Cloud computing is fast creating innovation, the testing issue is the main successfully impart scrambled in distributed computing. Despite the fact that user's direct uploads, the data in the cloud drop box without encryption. So the hacker easily hacks the data. Only distinct layers of security are available making it vulnerable to outside attacks. So we are using two layers of security and technique for encryption and decryption. The data in the cloud are stored in separate servers Deswarte et al. in [7] used RSA algorithm to check the file stored on a remote server. Using metadata functions the client can execute several challenges. Miller and Schwarz in [8] showed a technique for how dependable the information stored in the remotely in multiple server sites. They utilize the algebraic signature to block the files. Auditing of the public is discussed by Athens et al. [9] for protecting the data on entrusted store they used an RSA based homomorphism tag's function for auditing. C. Airways all at [10] they use a dynamic protocol function. it supports dynamic operations TPA is used for testing the data

Conclusion

How the data is covered, encrypted and verified using TPA and all this schemes are disused in this paper. Since this schemes user can be more confident on the cold storage. In this paper, we utilized an aggregate decryption key from this they can know that is accessing their data. The owner gets notified through the mail.

References

[1] Cheng-Kang Chu et al Deng Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage IEEE TRANSACTIONS ON PARALLEL & DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.

[2] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu, "SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), Vol. 7341, pp. 526-543, 2012.

[3] L. Hardesty, Secure computers aren't so secure.MIT press, http://www.physorg.com/news176107396.html, 2009.

[4] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for secure Cloud Storage," IEEE Trans. Computers, Vol. 62, no. 2, pp. 362-375, Feb. 2013.

[5] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared data on the cloud via Security-Mediator," Proc. IEEE 33rd Int'l Conf.Distributed Computing Systems (ICDCS), 2013.

[6] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng,"Dynamic Secure Cloud Storage with Provenance," Cryptographyand Security, pp. 442-464, Springer, 2012.

[7] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote Integrity Checking", In Proc. Of Conference on Integrity and Internal Control in Information Systems (IICIS'03), November 2003.

[8] T. Schwarz and E.L. Miller, "Store, forget, and check: using algebraic signatures to check remotely Administered storage", In Proceedings of ICDCS '06. IEEE Computer Society, 2006.

[9] G. Ateniese, "Provable Data possession at Untrusted Stores", Proc. 14th ACM Conf. Computer and Comm. Security (CCS' 07), 2007.

[10] C, Erway, A. Kuocu, C. Pamanthou, R.Tamassia, "Dynamic Provable Data Possession", Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), 2009.