An Empirical Model of Double Secure Method for out sourced Databases

[1]Yeluri Venky, [2]Suneetha Vesalapu
[1]Final M.Tech student, [2]Assistant professor
[1,2]Department of CSE, Avanthi institute of engineering and technology, Vizag, AP

Abstract:

In cloud service providers the storage is main task and very hard task. In third party server the data which is store by the owner have to maintain privacy over the data and defend from leakage. Single time encoding is very common process for providing security to the data. But considering the malicious attacks in the network channel we propose a framework for providing the double security to the data. We have implemented double encoding technique for providing more protection of data which is store in third party servers.And we introduced a double layer protection and we used symmetric key cryptographic techniques secure data. In this process data encrypted twice and store in cloud. Only authenticated users only access the information and we limited the user privileges over the cloud service.It supports more scalability of users. This contains secure public tags and verification process such as auditing. It reduces work load to server because simple verification process is only done by server all other security issued can done by auditing. Furthermore, our auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server.

1. INTRODUCTION

Distributed storage is a model of information storage in which the computerized information is put away in consistent pools, the physical storage traverses various servers (and frequently areas), and the physical environment is ordinarily possessed and oversaw by a facilitating organization. These distributed storage suppliers are in charge of keeping the information accessible and open, and the physical environment secured and running. Individuals and associations purchase or rent storage limit from the suppliers to store client, association, or application information.

Distributed computing, otherwise called 'on-interest processing', is a sort of Internet-based figuring, where shared assets, information and data are given to PCs and different gadgets on-interest. It is a model for empowering omnipresent, on-interest access to a mutual pool of configurable figuring resources.[1][2] Cloud registering and storage arrangements furnish clients and ventures with different capacities to store and process their information in outsider information centers.[3] It depends on sharing of assets to accomplish intelligence and economies of scale, like an utility (like the power framework) over a system. At the establishment of distributed computing is the more extensive idea of merged base and shared administrations. Distributed computing is a model for empowering omnipresent, helpful, on-interest system access to a common pool of configurable processing assets (e.g., systems, servers, storage, applications and administrations) that can be quickly provisioned and discharged with negligible administration exertion.

Advocates assert that distributed computing permits organizations to keep away from forthright base expenses, and concentrate on ventures that separate their organizations rather than on infrastructure.[4] Proponents additionally guarantee that distributed computing permits undertakings to get their applications up and running speedier, with enhanced sensibility and less upkeep, and empowers IT to all the more quickly conform assets to meet fluctuating and flighty business demand.[4] Cloud suppliers commonly utilize a "pay as you go" model. This can prompt surprisingly high charges if overseers don't adjust to the cloud evaluating model.. The present accessibility of high-limit systems, minimal effort PCs and storage gadgets and additionally the boundless selection of equipment virtualization, administration situated engineering, and autonomic and utility figuring have prompted a development in cloud computing. Companies can scale up as registering needs increment and afterward downsize again as requests reduction.

The principle empowering innovation for distributed computing is virtualization. Virtualization programming isolates a physical processing gadget into one or more "virtual" gadgets, each of which can be effectively utilized and figured out how to perform registering errands. With working system–level virtualization basically making an adaptable arrangement of numerous autonomous registering gadgets, unmoving figuring assets can be distributed and utilized all the more effectively. Virtualization gives the spryness required to accelerate IT operations, and diminishes cost by expanding foundation usage. Autonomic registering robotizes the procedure through which the client can procurement assets on-interest. By minimizing client association, robotization speeds up the procedure, lessens work costs and decreases the likelihood of human mistake.

II.RELATED WORK

Approaches closely related to our work have been investigated in three different areas: selective publication and broadcast of documents as well as attribute-based security and group key management. The database and security communities have carried out extensive research concerning techniques for the selective dissemination of documents based on access control policies. These approaches fall in the following two categories.[5]

1) Encryption of different subdocuments with different number of keys which are provided to users at the registration phase, and broadcast the encrypted sub documents to all users.

2) Selective multi-cast of different sub documents to different user groups and where all sub documents are encrypted with one symmetric encryption key.

The latter approaches assume that the users are honest and do not try to access the sub documents to which they do not have access authorization. Therefore, these approaches provide neither backward nor forward key secrecy. In the traditional approaches users are able to decrypt the sub documents for which they have the keys. However, such approaches require allow some keys be distributed in advance during user registration phase. This requirement leads difficult to assure forward and backward key secrecy[6] when user groups are dynamic with frequent join and leave operations.

In cryptography, the simple XOR cipher is a type of additive cipher,[1] an encryption algorithm that operates according to the principles:

A \oplus 0 = A,

A \oplus A = 0,

(A \oplus B) \oplus C = A \oplus (B \oplus C),

(B \oplus A) \oplus A = B \oplus 0 = B,

where \oplus denotes the exclusive disjunction (XOR) operation. This operation is sometimes called modulus 2 addition (or subtraction, which is identical).[2] With this logic, a string of text can be encrypted by applying the bitwise XOR operator to every character using a given key. To decrypt the output, merely reapplying the XOR function with the key will remove the cipher[7].

III.PROPOSED SYSTEM

In this proposed work we introduced double layer security method. We propose a new model which contains Cloud Service, user, auditor, and data owner.

Cloud Service: It is a third party service which contains large amount of database to store information. It allows data to store information by authenticated users.

User: He / She only have an access to read data when request to cloud.

Data Owner: He / She stores encrypted content and generate signature to the content. He is the owner of the stored content.

Auditor: He / She verifies the content in the cloud frequently, to check if content is secure or not. He can check file using the signature sent by cloud and Data owner.

Algorithm is as follows:

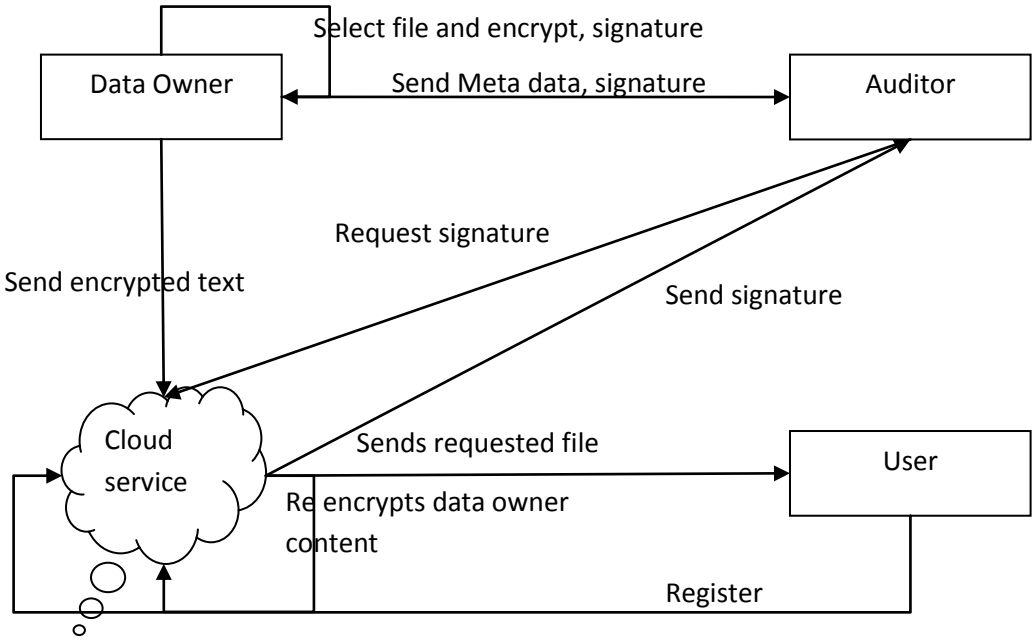
a) Initialization

Initially all users, Data owners register in the cloud service. For data owners the Cloud generate a secret key ‘sk’. And it is modified by a random value ‘r’ by doing simple arithmetic operation.

That modified key 'msk' is sent to data owner such as (msk,r). Data owner receives that modified key and reveal the modified key.

b) Storage and encryption

After generating of the key, Data owner selects a text file and encrypts that file content



using. SERPENT operates on a 4×4 column-major order matrix of bytes, termed the state have a larger block size and have additional columns in the state. The general SERPENT calculations are done in a special finite field. The key size used for anSERPENT cipher specifies the number of repetitions transformation rounds that convert the input is so called the plaintext. The final output called the cipher text. The numbers of cycles of repetition are as follows: 10 cycles for 128-bit keys per repetition,12 cycles for 192-bit keys per repetition, 14 cycles for 256-bit keys per repetition.

Each round consists of several processing steps and each containing four similar but different stages that includes one that depends on the encryption key itself. A sequence set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.In this process the auditor mainly involves mainly in the process of verification. Auditors have the signature sent by the data owner and request the cloud for stored file signature. In a cloud decrypts the encrypted content and generate signature and sent to auditor. Then auditor compares the signatures of data owner and cloud of requested file. If the signatures are same the files are secure, otherwise auditor conclude that file in the cloud is corrupted and sends status to data owner.

By using this process we can reduce the maximum leakage of data and man in the middle attacks in the network channel.In this proposed work we introduced double layer9 security method. We propose a new model which contains Cloud Service, user, auditor, and data owner.

Cloud Service: It is a third party service which contains large amount of database to store information. It allows data to store information by authenticated users.
User: He / She only have chance to read data when request to cloud.

Data Owner: He / She stores encrypted content and generate signature to the content. He is the owner of the stored content.

Auditor: He / She verifies the content in the cloud frequently, to check if content is secure or not. He can check file using the signature sent by cloud and Data owner.

Modules:

1. Cloud Service Provider
2. Secure Implementation
3. Auditing

Cloud Service Provider:

It provides data storage service and has enough storage space to maintain client's data and updates over database. Cloud service provider allows an authorized auditor to monitor the data components and instant mails can be forwarded to Data owner.Initially the data owner, user registers in cloud service provider. Then data owner requests to store his content in cloud service provider. Cloud authenticates data owner then data owner encrypts his file and send to cloud.

Secure Implementation:

Then cloud service re-encrypts the encrypted file and store in the cloud database. Data owner also generates the signature to his file using secure hash h(m) algorithm. Then send that signature to auditor. If any user wishes to read particular data owner file, user requests to cloud service provider then CSP sends response to user with an authentication code. Then user reads that requested file using authenticated code. For encryption and decryption purpose we used block cipher algorithms such as AES and Rijandael Algorithms, why because these two are similar type of algorithms and we use similar keys for these two algorithms. In data owner side AES algorithm is used for encryption and from cloud side we used Rijandael algorithm for encoding.

Auditing:

We introduced auditor as trusted member because frequent verification of the files in cloud. Data owner sends his file and there is no need to bother about his content. But the responsibility to secure his file is for cloud service provider. Due more scalability cloud should busy in communication with data owners and users management. It has more burdens to monitor all files in it.

So we introduces auditor in this architecture to regular monitoring of the files stored in cloud. Without leaking public information of the content such as keys and content of the file, auditor has to monitor or verify stored files. That what auditor checks the file content by given signatures of both data owner and cloud service provider. And data owner also send file details such as file unique Id, data owner id etc.

IV.CONCLUSION

In this paper we proposed a novel architecture for double secure method for cloud storage. It is mainly introduced on the idea of security of the data in cloud services. In this we used a symmetric cryptography for the data which is stored in the cloud databases. In this we introduced a architecture for cloud secure method for storage. It reduces work load to server because simple verification process is only done by server all other security issued can done by auditing. Furthermore, our auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server.

REFERENCES

[1] Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia (2009, Feb. 10). Above the clouds: A Berkeley view of cloud computing. EECS Dept. University of California, Berkeley, No.UCB/EECS-2009-28[Online].Available: http://radlab.cs.berkeley.edu/

[2] H. Takabi, J.B.D. Joshi, and G-J.Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, vol. 8, no. 6, 2010.

[3] R. Buyya, C. S. Yeo, and S. Venugopal, Market oriented cloud computing: vision, hype, and reality, for delivering IT services as computing utilities, Proc. 10th IEEE International Conference on High Performance Computing and Communications.

[4] Aafaq Ahmad Peerzada, Er.RishmaChawla," An Analytical Review of the Multimedia Data and Encryption Mechanism at Cloud Server" 10th IEEE International Conference on High Performance Computing and Cloud Security.

[5] Dalian, Daemen, Joan; Rijmen, Vincent (9/04/2003). "AES Proposal: Rijndael". National Institute of Standards and Technology.p.1.Retrieved 21 February 2013.

[6] Jump up^ John Schwartz (October 3, 2000). "U.S. Selects a New Encryption Technique". New York Times. China, Sept 2008.

[7] ^ Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, Mike Stay (May 2000). "The Twofish Team's Final Comments on AES Selection".

BIOGRAPHIES

VenkateshYeluristudying m.tech(software engineering) from avanthi institute of engineering and technology,vizagaffiliated to jntukakinada from 2013-2015. He completed b.tech(information technology) from narasaraopeta institute of technology,narasaraopet, affliated o jntukakinada from 2008-2012.

SuneethaVesalapu received her **b.tech** in computer science and engineering from vitam engineering college.presently she is working as assistant professor in computer science and engineering department in avanthi institute of engineering and technology,vizag. Her research interests include network security,data warehousing and data mining,rdbms.she has published 02 papers in international journals on data mining.