ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Anonymous access request matching mechanism with security and privacy considerations in Cloud Computing

Panigrahi Venkataramana
M.Tech (Software Engineering),
Department of Computer Science Engineering,
Sarada Institute of Science Technology and Management.

Ramesh Kumar Behara
Asst.Professor,
Department of Computer Science Engineering,
Sarada Institute of Science Technology and Management.

Abstract:

A cloud refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measured IT resources. The term originated as a metaphor for the Internet which is, in essence, a network of networks providing remote access to a set of decentralized IT resources. The moving of business data to the cloud means that the responsibility over data security becomes shared with the cloud provider. There are many users using cloud services which related to cloud computing.

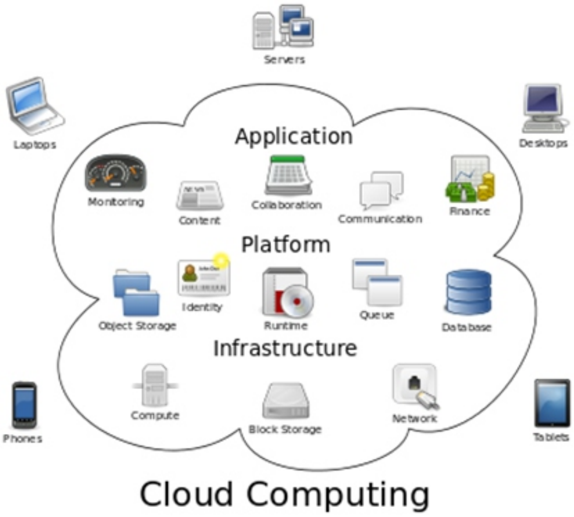
The data which is stored by many users are to be protected by cloud services only. In many situations user facing many problems due to collisions, low bandwidth, and server unavailability at the time of communication etc. Therefore we designed new methodology for the achieving these problems. It consists of a secure shared authority and the secure communication over the network.

Keywords:

Cloud computing, Communications, Nodes, security, Data Integrity, Privacy, Access Control.

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). dynamically assigned and reassigned according to consumer demand.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

To protect data privacy, confidential data has to be encrypted before outsourcing, so as to provide end-to-end data confidentiality assurance in the cloud. Data encryption makes effective data utilization a verychallenging task given that there could be a large amount of outsourced data files. Besides, in Cloud Computing, data owners may share their outsourced data with a large number of users, who might want to only retrieve certainspecific data files they are interested in during a given session. One of the most popular ways to do so is through keyword-based search.

This keyword search technique allows users to selectively retrieve files of interest and hasbeen widely applied in plaintext search scenarios. Unfortunately, data encryption, which restricts user's ability to perform keyword search and further demands the protection of keyword privacy, makes the traditionalplaintext search methods fail for encrypted cloud data. Ranked search greatly improves system usability by normal matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency).

Existing System:

In the cloud storage based supply chain management,there are various interest groups (e.g., supplier,carrier, and retailer) in the system. Each group owns itsusers which are permitted to access the authorized datafields, and different users own relatively independentaccess authorities.It means that any two users fromdiverse groups should access different data fields of thesame file.

Thereinto, a supplier purposely may want toaccess a carrier's data fields, but it is not sure whetherthe carrier will allow its access request. If the carrierrefuses its request, the supplier's access desire will berevealed along with nothing obtained towards the desireddata fields.

Actually, the supplier may not sendthe access request or withdraw the unaccepted request inadvance if it firmly knows that its request will be refusedby the carrier. It is unreasonable to thoroughly disclose the supplier's private information without any privacyconsiderations. Fig. 1 illustrates three revised cases toaddress above imperceptible privacy issue.

- **Case 1:** The carrier also wants to access the supplier'sdata fields, and the cloud server should inform eachother and transmit the shared access authority to theboth users;
- **Case 2:** The carrier has no interest on other users' datafields, therefore its authorized data fields shouldbe properly protected, meanwhile the supplier'saccess request will also be concealed;
- **Case 3:** The carrier may want to access the retailer'sdata fields, but it is not certain whether the retailerwill accept its request or not. The retailer's authorizeddata fields should not be public if the retailerhas no interests in the carrier's data fields, and thecarrier's request is also privately hidden.

Disadvantage: Previous System does not have the option of granting/revoking data access

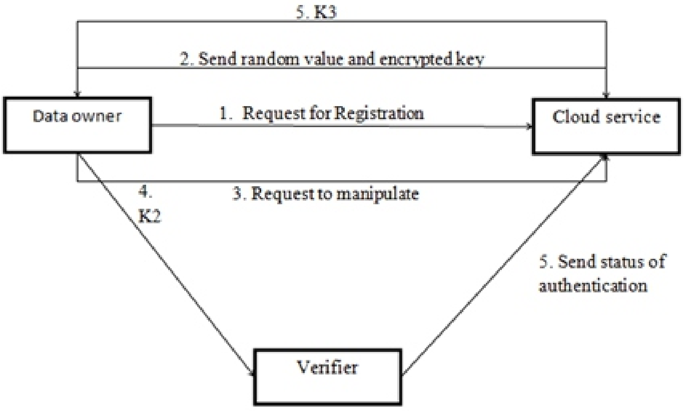
Proposed System:

In our work we proposed a methodology and it contains two parts such as Authentication and secure communication. In our work there are three major roles such as Data owner, Auditor, cloud service. Data owner selects data to upload in the service in encoded format and he can manipulate uploaded file or remove his file. Auditor and the cloud service provider both authenticate the data owner.

Advantage: Here we proposed the secured system and data owner can decide whether the user can access the system or not.

Problem Statement: In our model, privacy is accomplished by encrypting the data it can prevent the un authorized access.

Scope: We are going to raise the privacy level of the data owner and the confidentiality of the data by providing access to users The below shown the architecture of our methodology.


5. K3
2. Send random value and encrypted key
Data owner
1. Request for Registration
Cloud service
4. K2
3. Request to manipulate
5. Send status of authentication
Verifier

Architecture:

Modules :

1.Owner
2.User
3.Access Control
4.Cloud Service Provider
5.Encryption & Decryption
6.File Download
7.Trusted Third Party

Owner Registration: In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.

Owner Login: In this module,any of the above mentioned person have to login,they should login by giving their emailid and password .

User Registration: In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

Access Control: Owner can permit access or deny access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not allow, user can't able to get the data.

Encryption & Decryption: Here we are using this aes_encrypt & aes_decrypt for encryption and decryption. The file we have uploaded which has to be in encrypted form and decrypt it

File Upload: In this module Owner uploads the file(along with meta data) into database, with the help of this metadata and its contents, the end user has to download the file. The uploaded file was in encrypted form, only registered user can decrypt it.

File Download: The Authorized users can download the file from clou database.

Cloud Service Provider Registration: In this module , if a cloud service provider(maintainer of cloud) wants to do some cloud offer , they should register first.

Cloud Service Provider Login: After Cloud provider gets logged in, He/ She can see Cloud provider can view the files uploaded by their clients.
Also upload this file into separate Cloud Database.

Ttp (Trusted Third Party) Login:

In this module TTP has monitors the data owners file by verifying the data owner's file and stored the file in a database .Also ttp checks the CSP(CLOUD SERVICE PROVIDER),and find out whether the csp is authorized one or not.

Authentication Method:

Initially data owner request for registration to cloud service. Then service provider sends random value and the encrypted secret key to the data owner as shown below:
Ack(Di)=Msg(r,enc(sk))
After retrieving of the data from the cloud service provider, data owner upload or manipulate his file after authenticate him as shown below.

If the user is an authorized user, he/she

Auth1=fist part (Enc(Dec(Sk))/2)
Auth2=Second part(enc(Dec(sk))/2)

Auth1 code sent to service and second to verifier. If the both authorities approved his authentication parameters then only he allowed to upload or manipulate the data in cloud service.

For Data encryption and decryption We used Rijandael

algorithm as shown below:

ES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware.[9] Unlike its predecessor DES, RIJNDAEL does not use a Feistel network. RIJNDAEL is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

RIJNDAEL operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most RIJNDAEL calculations are done in a special finite field.The key size used for an RIJNDAEL cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:
10 cycles of repetition for 128-bit keys.
12 cycles of repetition for 192-bit keys.
14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

High-level description of the algorithm

KeyExpansions: round keys are derived from the cipher key using Rijndael's key schedule. RIJNDAEL requires a separate 128-bit round key block for each round plus one more.

InitialRound:

AddRoundKey:

each byte of the state is combined with a block of the round key using bitwise xor.Rounds

SubBytes:

a non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows:

a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

MixColumns:

a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey
Final Round (no MixColumns)
SubBytes
ShiftRows
AddRoundKey.

Psuedo code:

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in

AddRoundKey(state, w[0, Nb-1]) // See Sec. 5.1.4
for round = 1 step 1 to Nr–1
SubBytes(state) // See Sec. 5.1.1
ShiftRows(state) // See Sec. 5.1.2
MixColumns(state) // See Sec. 5.1.3
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
end
```

CONCLUSION:

In this work, we have distinguished another protection challenge amid information getting to in the distributed computing to accomplish security protecting access power offering. Validation is created to ensure information privacy what's more information respectability. Information namelessness is accomplished following the wrapped qualities are traded amid transmission. Client security is upgraded by nameless access demands to secretly advise the cloud server about the clients' access wants. Forward security is acknowledged by the session identifiers to keep the session relationship. It shows that the proposed plan is conceivably requisitioned improved protection safeguarding in cloud applications.

References:

[1]Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member, IEEE, and Laurence T. Yang, Member, IEEE, Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing, Parallel and Distributed Systems, IEEE Transactions on (Volume:PP , Issue: 99)

[2] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2012.

[3] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE INFOCOM. , pp. 441–445, 2010.

[5] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[6] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in CloudCom, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

[7] C. Gentry, "A fully homomorphic encryption scheme,"Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[8] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in TRUST, ser. Lecture Notes in Computer Science, vol. 6101. Springer, pp. 417–429, 2010.

[9] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B. S. Lee, "Trust cloud: A framework for accountability and trust in cloud computing," HP Technical Report HPL-2011- 38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[10] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of DataFo rensics in Cloud Computing," in ACM ASIACCS, pp. 282–292, 2010.

[11] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

[12] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," IEEE Computer, vol. 43, no. 6, pp. 79–81, 2010.

[13] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multiowner settings," in SecureComm, pp. 89–106, 2010.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.

[15] G. Wang, Q. Liu, and J. Wu, "Hierarchical attributebased encryption for fine-grained access control in cloud storage services," in ACM CCS, , pp. 735–737, 2010.

[16] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.

Author Details :

Panigrahi.venkataramana is a Student in M.Tech(SE) in Sarada Institute of Science Technology And Management, Srikakulam. He Received his B.Tech(CSIT) from Sarada Institute of Science Technology And Management(SISTAM), Srikakulam. JNTU Kakinada Andhra Pradesh.

Ramesh kumar Behara is working as Asst.professor in Sarada Instituteof Science, Technology And anagement,Srikakulam, Andhra Pradesh. Hereceived his M.Tech (CSE) from Sarada Institute of Science, TechnologyAnd Management,Srikakulam, Andhra Pradesh. JNTU Kakinada AndhraPradesh. His research areas include Network Security