International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 01 | Jan 2020 www.irjet.net p-ISSN: 2395-0072

A Research paper on Block Design-based Key Agreement for Group Data Sharing in Cloud Computing

Wajiha Nausheen[1] & Shital Gaikwad[2]

[1]PG Student, Department of Computer Science and Engineering, Mathoshri Pratishthan Group of Institutions, Khupsarwadi, Nanded, Maharashtra, India
[2]Associate Professor, Department of Computer Science and Engineering, Mathoshri Pratishthan Group of Institutions, Khupsarwadi, Nanded, Maharashtra, India

---

Abstract - *Cloud computing is evolving and considered next generation architecture for computing. Typically cloud computing is a combination of computing recourses accessible via internet. Historically the client or organizations store data in data centres with firewall and other security techniques used to protect data against intrudes to access the data. However in cloud computing, since the data is stored anywhere across the globe, the client organizations have less control over the stored data. To build the trust for the growth of cloud computing the cloud providers must protect the user's data from unauthorized access and disclosure.*

Today, use of cloud computing is rapidly growing for several purposes, mainly for large data storage and sharing data in clouds. Here, users can share data for dynamic groups with cost-effectively. Membership is frequently changing in a cloud. The Existing system is using the protected (secure) commutation channel for data sharing. This implementation is difficult for practice. Still, the existing system is suffering from collusion attack and insecure key distribution with a single cloud. There is no assurance of the data confidentiality and accessibility. In the proposed system, multiple cloud services are used to store data. The System is proposing a safe way for key distribution without using any protected communication channels, and the user can safely get their private keys from group administrators (managers).Any users in the gathering can use the source in the cloud and denied users cannot get to the cloud once more. The system provides fine-grained access control.

Also, the system supports the anti-collusion attack with an untrustworthy cloud. Our system is proposing two levels of encryption techniques and a file is stored in a split format on multiple clouds in different groups using a hybrid cloud. The system is providing secure revocation

Key Words: Key agreement protocol, symmetric balanced incomplete block design (SBIBD), data sharing, cloud computing

1. INTRODUCTION

In cloud computing, the cloud service providers offer single or multiple cloud services for storing and sharing data securely among users i.e. Amazon service S3. Cloud providers offers large storage space with abstraction for simplicity of the user. The membership in the cloud is frequently changing and because of this, security-preserving are turned into a challenging issue in the cloud. Company employees in the same department can share and store files in the cloud. However, here is a significant risk to the confidentiality of those stored files. For security purpose, it is necessary to encrypt data before uploading files in the cloud .These schemes do not support for secure data sharing for dynamic groups. Some systems have used techniques for securing data sharing called cryptography among multiple group members in an untrustworthy cloud .But these systems additionally experiences a cost overheads and security risks. These systems are not supported to dynamic group concept.re not supported to dynamic group concept.

1.1 Background:

In some systems, combined approaches of key policy attribute based encryption, proxy re-encryption, and lazy re-encryption is used to achieve fine-grained data access control without disclosing data contents. Other system uses the group signatures and cipher text-policy attribute based encryption techniques. But these systems does not support to efficient user revocation. It breaches security. The multi-owner schemes use the attribute-based techniques. If any owner revokes from an application, it leads to security issues. This approach is not safe for data sharing. Many approaches based on privacy-preserving policies in public clouds. These approaches are easily suffering due to collusion attack. The Existing approach supports secure data sharing scheme for dynamic groups in a single cloud. The scheme uses attribute-based techniques. It does not support protected/secure user revocation. The proposed system uses role-based techniques for secure data sharing and key distribution for dynamic groups by taking the advantage of multiple clouds. In multiple clouds, storage space is again partitioned into groups. The files get partitioned and then store in multiple groups with two level of encryption. The system Supports anti-collision attack and secure user revocation. Our system overcomes cost overhead. Our approach removes a space overhead by using the concept of the virtual storage server. Here, the time and space constraints are applied. If the space of storage became full, stored data is automatically transferred to the virtual server according to the time and space constraint.

1.2 Motivation:

The Aim of this project is to propose a scheme that provides the security, data sharing in multiuser cloud. To Calculated the Fault Tolerances and fault Detection of user Side if hacker hack any file of owner tolerance level increases.

- Data Security in Cloud.
- Mechanism to store data in cloud
- Mechanism to fetch data from cloud
- Access Control Lists with respect to roles on Data
- Performance improvement with using lightweight and flexible encryption mechanism to secure data from cloud providers.

1.3 GOALS /OBJECTIVES

Authors wanted to show that is criticism about privacy in cloud model, because of the fact that administrator have access to data stored in the cloud. They can unintentionally or intentionally access the client data. Traditional security or protection techniques need reconsideration for cloud. Except for private cloud where organization does not have control over the equipment, the progress of cloud is seems little slow, because organizations think instead of compromising on the security of the data, they are still willing to invest in buying private equipment to setup their own infrastructure. Security issues which are of concern to the client can be classified into sensitive data access, data segregation, bug exploitation, recovery, accountability, malicious insiders, and account control issues. Like different disease have different medicines, different cloud security issues have different solutions, like cryptography, use of more than one cloud provider, strong service level agreement between client and cloud service provider. Heavy investment is needed to secure the compromising data in cloud. Following are some of the concerns.

A. System Complexity: Compared to traditional data center the cloud architecture is much more complex. Therefore while considering security, security of all these components and interaction of these components with each other needs to be addressed.

B. Shared Multi-tenant Environment

Since the cloud needs to provide service to millions of client, a logical separation of data is done at different level of the application stack. Because of which attacker in the face client can exploit the bugs gaining access to data from other organizations.

C. Internet-facing Services: The cloud service which is accessed over the internet via browser, the quality of service delivered on the network is another concern.

D. Loss of control: As the data of client is stored anywhere across the world control loss over physical, Logical of system, and alternative control to client's assets, mismanagement of assets Are some additional concerns.

2. PROPOSED SYSTEM ARCHITECTURE

In Block level Design there are four module owner, user and Admin and Cloud Service Provider. User entry in application First user Register and Login then admin get activated the user and given the token after entre the token user login successfully after login user Search the owner file and cloud Services Provider given the Key in format of KASE. If user Entre the Wrong key (KASE) then level of fault Tolerances is level is increases and that level goes up to three then owner known the user information and if owner block the that user then after words user block from particular owner the user are not able to get file of particular owner

Advantages:

1. The scope of this project is to propose a scheme that provides the anti-collusion data sharing in multiuser cloud.
2. In cloud Computing Fault Detection from user side.
3. In cloud Computing Fault Tolerances and Data Owner.
4. Provide two level securities.
5. Cloud computing reduces the response time and running time of job, also minimizes the risk in deploying application, lowered cost of deployment, and decreasing the effort and increasing innovation
6. Increased Throughput: Cloud makes use of thousands of servers to finish an assignment in reduced time unit verses the time required by a solitary server

The system architecture is shown below,

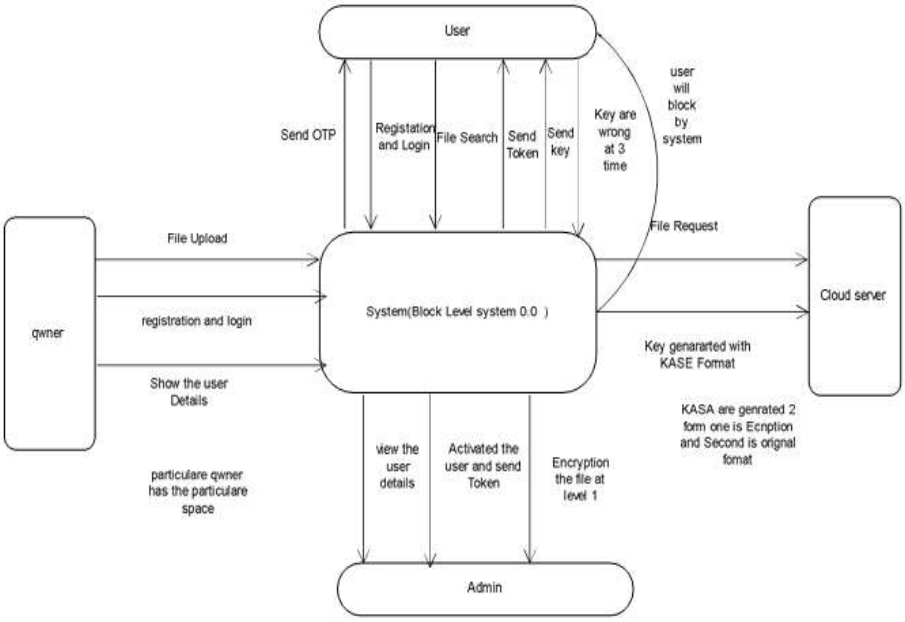


Fig -1: Proposed System Architecture

3. RELATED WORK

The AES cipher is part of a family known as block ciphers, which are algorithms that encrypt data on a per-block basis. These "blocks" which are measured in bits determine the input of plaintext and output of ciphertext. So for example, since AES is 128 bits long, for every 128 bits of plaintext, 128 bits of ciphertext are produced. Like nearly all encryption algorithms, AES relies on the use of keys during the encryption and decryption process. Since the AES algorithm is symmetric, the same key is used for both encryption and decryption. AES operates on what is known as a 4 x 4 column major order matrix of bytes. Here is how the cycles break down. A) 10 rounds are required for a 128-bit key. B) 12 Rounds are required for a 192-bit key. C) 14 Rounds are required for a 256-bit key.

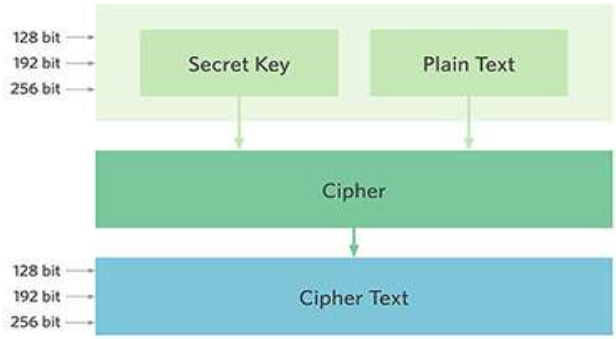


Fig -2: AES Algorithm

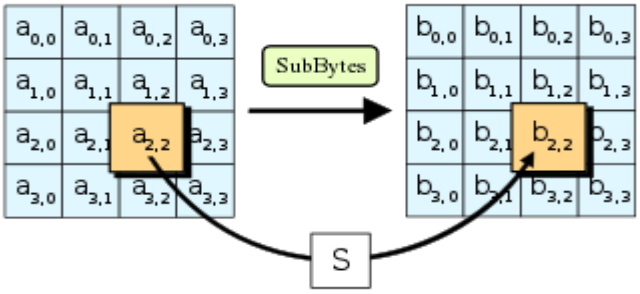
Broadly speaking the encryption/decryption can be done via symmetric key or asymmetric key in symmetric algorithms, both parties share the secret key for both encryption/decryption, and from privacy perceptive it is important that this key is not compromised, because cascading data will then be compromised. Symmetric encryption/decryption requires less power for computation. On the other hand asymmetric algorithms use pairs of keys, of which one key is used for encryption while other key is used for decryption. Generally the private key is kept secret and generally held with the owner of data or trusted 3rd party for the data, while the public key can be distributed to others for encryption. The secret key can't be obtained from the public key

3.1 Key Generation Algorithm:

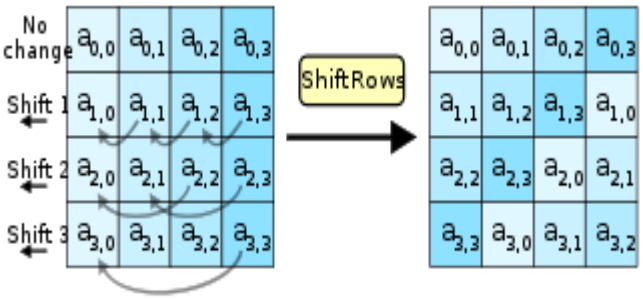
```
Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])
  Begin
      byte state[16]; state = in;
      AddRoundKey(state, round_key[0]);
      for i = 1 to Nr-1 stepsize 1 do SubBytes(state);
      ShiftRows(state);
      MixColumns(state);
      AddRoundKey(state, round_key[i]);
      end for SubBytes(state);
      ShiftRows(state);
      AddRoundKey(state, round_key[Nr]);
  End
```

3.2 High-level description of the algorithm

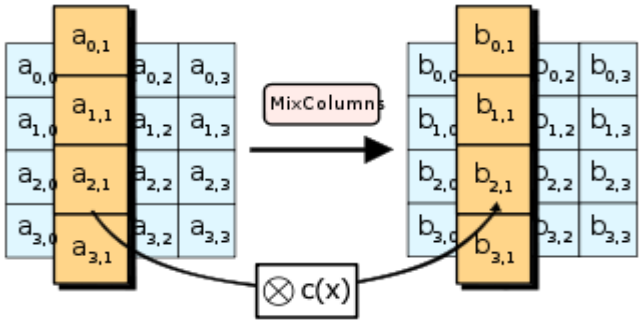
1. **KeyExpansions**—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. **InitialRound**
    1. **AddRoundKey**—each byte of the state is combined with a block of the round key using bitwise xor.
3. **Rounds**
    1. **SubBytes**—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. **ShiftRows**—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    3. **MixColumns**—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. **AddRoundKey**
4. **Final Round (no MixColumns)**
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey.



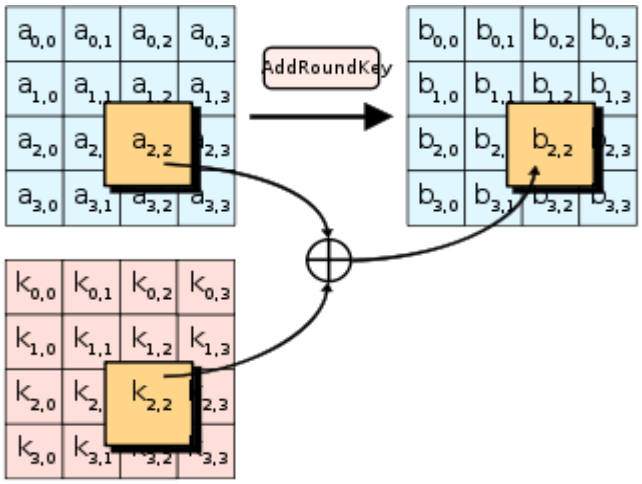
In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.



In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.



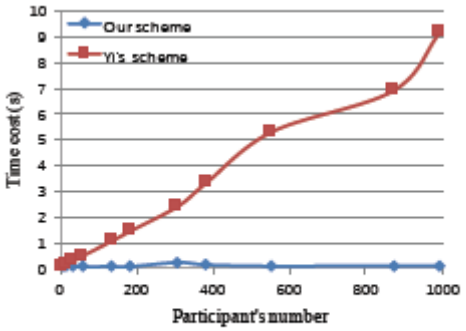
In the MixColumns step, each column of the state is multiplied with a fixed polynomial



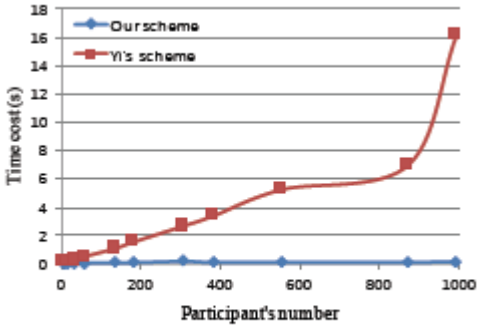
In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XORoperation (⊕)..

4. CONCLUSION

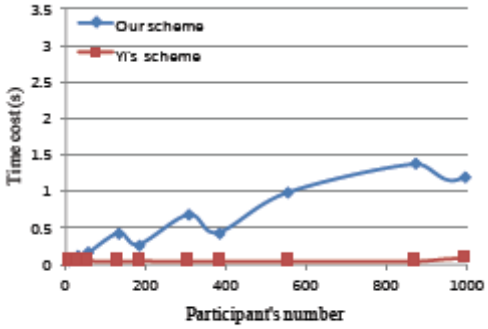
We have made comparison on bases of 3 phases with old method and our method. It can be clearly seen that at initial phase the time cost required is less than the previous one. Moving towards 2nd phase we have made comparison on basis of key agreement phase. In this phase also the we have been proved as most time effective. Again with the last phase you can see that we had given more strong authenitication process as we have provided TPS for all task.



(a) Initial phase



(b) Key agreement phase



(c) Authentication phase

In Cloud Computing as we provide a privacy-preserving auditing protocol . It enables an external auditor to audit user's cloud data without learning the data content. This scheme is the first to support scalable and efficient privacy preserving public storage auditing in Cloud. Specifically, it achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner. It achieves two end data security level so it's more secure.

REFERENCES

[1] L. Zhou, V. Varadharajan, and M. Hitchens, "Cryptographic rolebased access control for secure cloud data storage systems," Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 2381–2395, 2015.

[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with secure network coding," in IEEE INFOCOM, 2014, pp. 673– 681.

[3] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," Journal of Communications and Networks, vol. 14, no. 6, pp. 682–691, 2012.