iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VIII **Month of publication:** August 2020

DOI: https://doi.org/10.22214/ijraset.2020.30859

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

Client Centric Proxy Re-Encryption for Outsourcing Data in the Cloud

Sheelavathi A[1], Hariharan S[2], Pradeep A[3], Sushrutan G S[4]
[1]*Assistant Professor Information Technology,Saranathan College of Engineering, Trichy.*
[2]*Information Technology, Saranathan College of Engineering, Trichy.*

Abstract: Data sharing in cloud computing is depriving user'direct control over the outsourced data, which inevitably raises security concerns and challenges ... Another way to think of is to allow data owners to define access policies and encrypt the sharing data with the attribute-based encryption under the access policies, only authenticated users whose attributes matching their policies can decrypt the cipher text ... However, here also data owner needs to download, decrypt and re-encrypt the requested data in case data access policies change dynamically and frequently.Extra computation cost and communication overhead have been introduced to the data owner ... Another way to think of is to allow data owners to define access policies and encrypt the sharing data with the attribute-based encryption under the access policies, only authenticated users whose attributes matching their policies can decrypt the cipher text

I. INTRODUCTION

When one is simply too busy to accommodate all his encrypted files, he may need to delegate his decryption rights to someone he trusts. This delegation of the ability to decrypt the cipher text is easily done if the delegator is online – simply decrypts the cipher text and re-encrypts the plaintext with the general public key of whom he trusts. However, this can be not always practical, for the delegator might not be online all the time And, it's undesirable to only disclose the key key to some un trusted server to try and do the transformation of the cipher text. to resolve the above mentioned problems, at Eurocrypt'98, Blaze, Bleumer and Strauss firstly proposed the concept of proxy re-encryption (PRE). in an exceedingly PRE scheme, a semi-trusted proxy with some additional information (re-encryption key, which is computed by the delegator in advance) can convert a cipher text computed under Alice's (delegator's) public-key into one intended to Bob (delegatee) with the identical plaintext. the elemental property of proxy re-encryption schemes is that the proxy isn't fully trusted..

II. CLOUD COMPUTING

Cloud computing is essentially a service oriented architecture rendering easy accessibility to any or all who make use of it. the necessity of computation power rendered by the machines is on a nonstop hike nowadays. The CPU computation power is boosting twice for each 3 years. However size of the files keeps increasing also in an incredible rate. 20 years ago, the common format is barely computer file. Later, computer can handle the graphics well, and play some calibre movies

A. Characteristics Of Cloud

Cloud computing demonstrate the following key characteristics:

1) *Agility:* The resources are re-provisioned by the system to rectify users' ability. The necessities are altered in step with the customer's requests.
2) *Application Programming Interface (API):* It is kind of like the normal programme which facilitates interaction between humans and computers. the appliance Programming interface enables the mechanism to interrelate with cloud software Representational State Transfer (REST)-based APIs is employed in cloud computing systems.
3) *Cost:* To convert the resources overheads to functioning leak then the system using open-cloud liberation model. The resource supposedly reduces the obstacles, as another of leveraging the tools and software for once the infrastructure use the services provided by the third party.
4) *Device and Site Independence:* The user is allowed to access the system using applications programme without considering location or what device the system use. The communications is provided by the intermediary and in off-site. The user can contact the possessions from somewhere when concerning to the web.
5) *Maintenance:* Rather than installing the resources on the users system the resources are often accessed from anywhere in any location. it's easy for the punter to preserve the records within the cloud.

6) *Multi-tenancy:* Numerous patrons use the similar open cloud. together with the massive group **of** punters, they allow the sharing of possessions and expenditures.
7) *Performance:* The loosely coupled architectures are constructed because the system interface using the net services. The performance of the system is monitored and consistency is to be maintained.
8) *Reliability:* The multiple redundant sites are accessed by several users simultaneously. It provides cloud computing suitable for business endurance and tragedy recovery.
9) *Scalability and Elasticity:* The resources are provided with none interruption to the users' request. The VM start-up time varies by VM type, location, operating systems and cloud providers.
10) *Security:* When data is scattered over a broader region or over a greater number of strategies yet as in multi-leaseholder systems shared by impertinent users then the intricacy of security is greatly increased.

B. *Types of Cloud Services*

1) *Infrastructure as a service (IaaS):* The customer can access the providing requests, data storage, networks, and other essential computing resources. Consumer is ready to arrange and sprint random software, together with the software package and application. The cloud infrastructure isn't managed and controlled by the buyer but they'll access software package, storage, organized applications
2) *Platform as a service (PaaS):* The qualifications afforded to the tip user is to rearrange onto the cloud communications purchaser created or acquired request created using programming expression and mechanisms reinforced by the contributor. The end user doesn't manage or control the elemental cloud communications including network, servers, operating systems, or cupboard space, but has control over the arranged applications and possibly product hosting location patterns.
3) *Software as a service (SaaS):* The facility presented to the tip user is to utilize the contributor's products running on the cloud transportation. The appliances are available from diverse punters approach through a skinny client crossing point like an online browser i.e., web-based email. The end user doesn't manage or control the essential cloud transportation including system, servers, operating systems, cupboard space, or maybe soul function capacity.

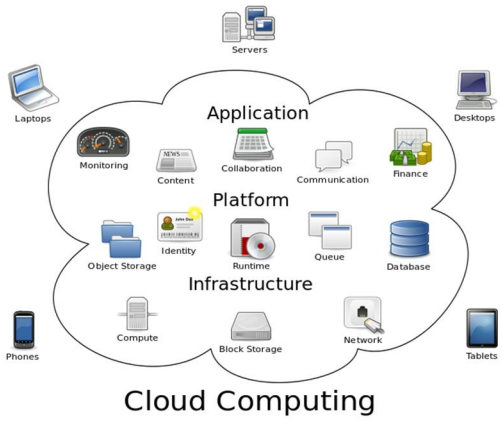


Figure: 1.3.

C. *Types Of Cloud Services*

1) *Advantages of Cloud Computing*

a) No capital investment needed for technology infrastructure.
b) No in-house man power needed to regulate over the technology infrastructure.
c) Pay just for recourses that we use (utility computing).
d) Used through an online browser as if it's a locally installed program.

2) *Disadvantages of Cloud Computing*

a) *Privacy* - No guaranteed since Cloud Service Provider can monitor your activities.
b) *Data Security* - Cannot guarantee misuse of information at data centers.
c) *Data Theft* – Hacking is on the rise and every one data is exposed on the web.
d) *Internet Connectivity* - Low Speed or Downtime would impact productivity.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

D. How Does Cloud Computing Work

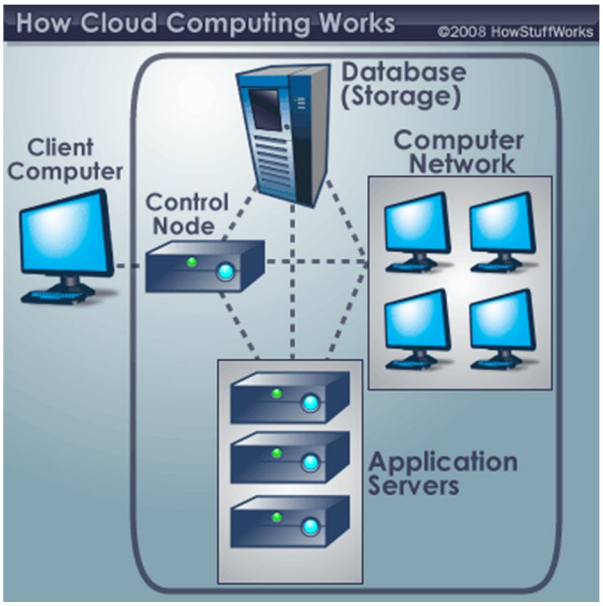


Figure .1.5.

E. Working of Cloud Computing

Cloud computer works by hosting your information on computers 'out there' 'in the cloud'. The cloud is largely a batch of computers called data centers or servers that hold your information (files, images, videos, etc) and may be located anywhere. You're working during a cloud because you don't must store software or files on your own computer.

Because all of the various servers are running together in cloud computing, one application can have the pc power of the many servers. this enables something like Facebook to run. Imagine trying to host Facebook on your laptop. It just wouldn't work.Therefore, the cloud brings together an outsized number of computers to work one application. And anything that's stored anywhere apart from your local hard drive—on your computer—is labeled as being within the clouds.

III. EXISTING SYSTEM

A. Type Based PRE provides semantic security and cipher-text privacy control but on the opposite hand encoding operations over encrypted messages isn't possible limiting its widespread use.

B. Key-Private PRE provides security against Chosen cipher-text Attack but the privacy proof of this scheme is tougher than Chosen plaintext attack. Identity-based PRE is secure against an adaptive CCA but it's difficult to search out such constructions for the algorithm that are multi-use, efficient and CCA secured.

C. Time based PRE could be a newer modification of PRE schemes which provides a scalable user revocation and reduces the workload of information owners. the key disadvantage of this scheme is that it require s the effective fundamental quantity to be same for all attributes related to the user..

IV. PROPOSED SYSTEM

A. Client Centric Proxy Re – Encryption

Client centric or User Centric proxy re-encryption can step in to supply a position or user. The platform creates a re-encryption token off of the general public key of the entity with whom its customers want to share data. That token can then be uploaded to the cloud where the third party can access it — successively enabling them to decrypt and access the information.

Ensuring compliance with regulations round the processing of sensitive data

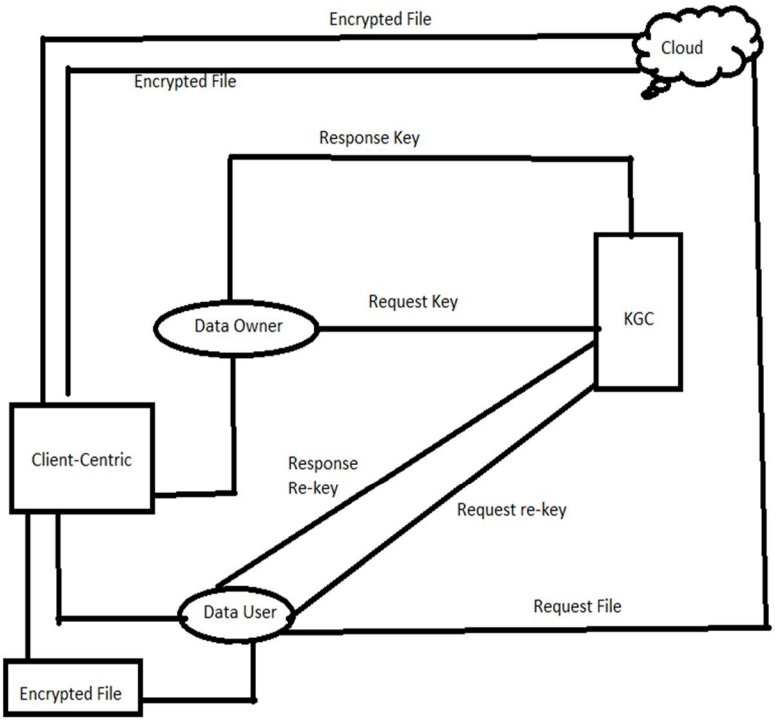
B. Merits

1) Cloud enablement

2) No Computational Overhead

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VIII Aug 2020- Available at www.ijraset.com

V. SYSTEM ARCHITECTURE



VI. MODULES

A. File Upload Module

When the client wants to upload a go into the cloud the client provides its Id together with the file to be uploaded. Cloud performs the EXOR operation during which the client's file is EXORed with the respective seed block of the client. the first file is stored within the main cloud and therefore the EXORed file is stored within the backup cloud. This information is updated within the proxy server. Response message is delivered to the user.

B. Key Generation

Key generation is that the process of generating keys for cryptography. The secret is wont to encrypt and decrypt data regardless of the data is being encrypted or decrypted. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as 3des).

C. User Module

The user has wanted to work out the file. The user has sent to asking for owner. The owner accepts the request then the file can view. The user using the client centric software

D. Client Centric

Client centric or User Centric proxy re-encryption can step in to supply a foothold or user. The platform creates a re-encryption token off of the general public key of the entity with whom its customers want to share data. That token can then be uploaded to the cloud where the third party can access it — successively enabling them to decrypt and access the information.

VII. PSUEDO CODE

1) Step 1: Get the key from Key Generation Centre.
2) Step 2: Encrypt the file and store in cloud.
3) Step 3: Get a key from KGC and encrypt the file in the cloud.
4) Step 4: When the user needs the file, get the key and decrypt the file in cloud and send it to the user.

VIII. IMPLEMENTATION

Output Rephrased/Re-written Text When one is just too busy to house all his encrypted files, he might need to delegate his decryption rights to someone he trusts. This delegation of the ability to decrypt the cipher text will be easily done if the delegator is online – simply decrypts the cipher text and re-encrypts the plaintext with the general public key of whom he trusts. However, this can be not always practical, for the delegator might not be online all the time.

A. Purpose

Secure sharing of sensitive encrypted data" — with multiple third parties, be it a customer, partner, supplier or perhaps a regulator. CC-proxy re-encryption technology enables it to give customers the power to manage access controls without having to supply full access to the info — which means it can remove any single point of failure

B. Scope

File size is increasing but the algorithms don't improve such a lot. Moreover, newer format always require more complicated decode algorithms and make the time interval longer. the sole thanks to greatly speed up the method is make the duty parallel running on different machines

IX. CONCLUSION

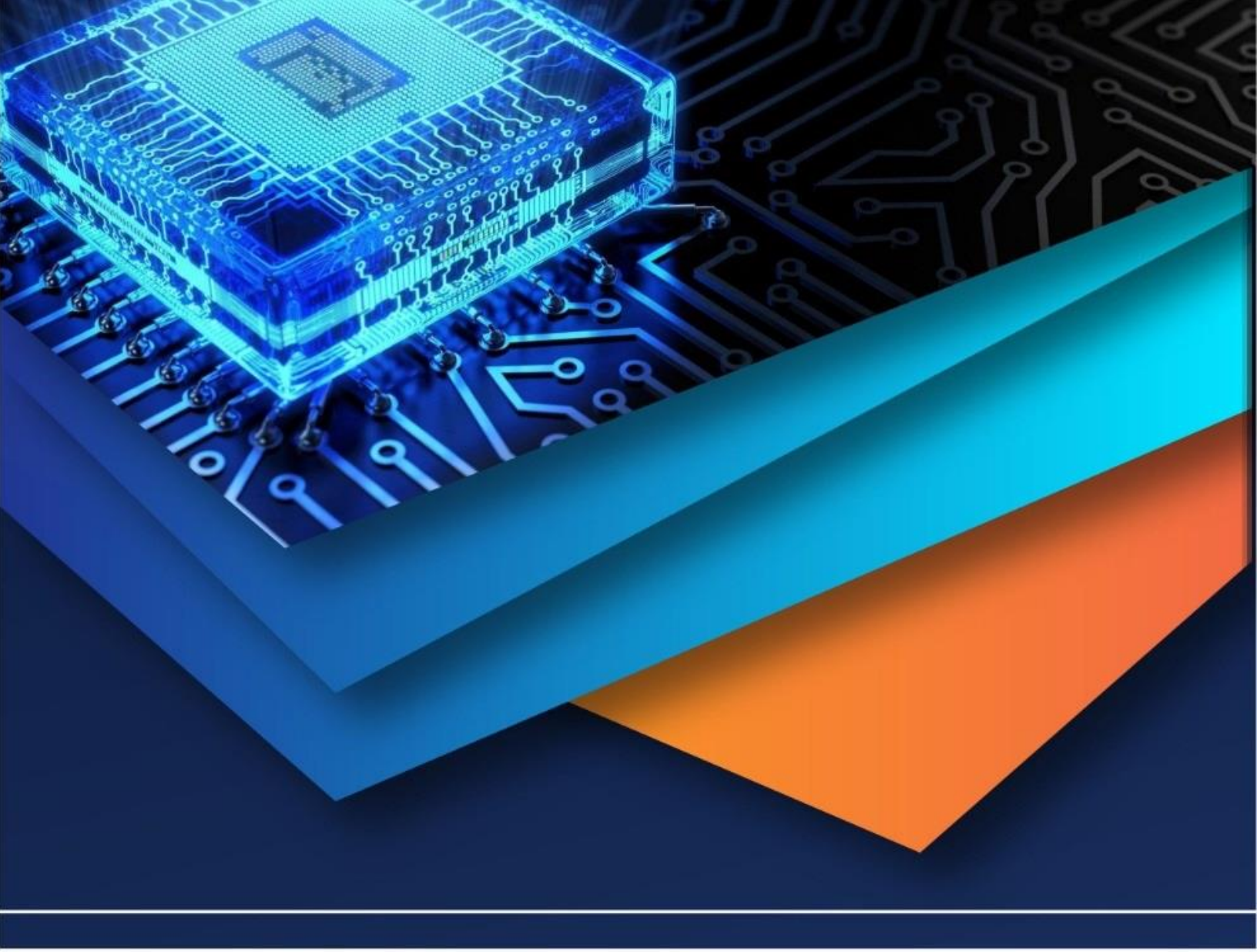
In this paper, we introduce a brand new cryptographic primitive, called autonomous path proxy re-encryption, which is motivated by the strain in several potential applications. Not only will we first advance the concept of delegator autonomous path proxy re-encryption, but also we provides a concrete construction of an IND-CPA secure scheme under this idea. We note that such scheme combines the advantage of a single-hop PRE and a multi-hop PRE, in other words, CCPRE provides far better fine-grained access control to the delegation path than the standard multi-hop PRE.

X. FUTURE ENHANCEMENT

New enhancement of this project is to scale back the scale of the backup cloud which makes it cost efficient. This project is meant for single users accessing the cloud,it will be enhanced to support cloud in an organisation.
In this project the protection is ensured by seed block algorithm which performs EXOR operation and encrypts the file and stores it within the backup cloud. the protection will be further enhanced by adding additional encryption techniques before storing it within the backup cloud.

REFERENCES

[1] Chintureena Thingom ,September 2014" A Study on Tools for Cloud Disaster Management"
[2] Kruti Sharma, Kavita R Singh, November 2012 "Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review". Noriharu Miyaho, Yoichiro Ueno, Shuichi Suzuki, Kenji Mori , August 2010 "Study of a Secure Backup NetworkMechanism for Disaster Recovery Practical NetworkApplications".
[3] Tanay Kulkarni **,** Krupali Dhaygude**,** Sumit Memane**,** Onkar Nene**"** October 2014 "Intelligent Cloud Back-Up System **".**
[4] Yoichiro Ueno, Noriharu Miyaho, Shuichi Suzuki,Muzai Gakuendai, July 2011 "Disaster Recovery System and Practical Network System Applications".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY