Shared Authority Based Privacy Preserving Authentication in Cloud Computing: A Review

[1]Prasad Arun Kadam, [2]Prof. Umakant Mandawkar
[1]Student, [2]Assistant Professor
[1]Computer Science and Engineering,
[1]School of Engineering and Technology, Sandip University, Nashik, India

Abstract : Distributed computing gives helpful approach to information sharing for clients. Yet, at some point clients may need to redistributed the common information to cloud server however it contain profitable data. Security has dependably been a major concern with regards to information partaking in distributed computing. Along these lines it is important to put cryptographically improved access control on the common information. The paper examine about a promising cryptographical crude for information partaking in cloud which is Identity-based encryption. We initially present the revocable-stockpiling character based encryption plot which gives both forward and in reverse security of ciphertext. At that point we will have look at all the procedures that have been utilized for usage of character based encryption so for. At long last we close the paper.

Index Terms **- Cloud Computing, Data Sharing, Identity-Based Encryption, Revocation.**

I. INTRODUCTION

Distributed computing is the term broadly utilized for a lot of PCs or generally disseminated gadgets which can share assets for successful processing needs. Distributed computing frameworks are valued according to the use thickness per client. The innovation can be effectively conveyed for across the board applications whether to execute an application to share photos to numerous clients or to create complex IT arrangements. The principle highlight of this sort of frameworks is that they don't include high speculation costs for equipment. This sort of equipment is kept up and facilitated by increasingly competent associations like Amazon. The advantage of such frameworks for engineers are that they don't force support expenses to the designers. On the client end the advantages can be recorded as they can appreciate the advantage of adaptable valuing framework.*Benefits of Cloud Computing*.

1) Trade capital cost for variable cost The client and the engineers pay for the measure of assets they are to utilize. This spares the pointless excess of assets and cost before the items are really conveyed and even after that.

2) Benefit from monstrous economies of scale Lower use based estimating plans have more achievement in targetting a wide scope of clients. This is on the grounds that the valuing plans are intended to accomodate all sizes of uses fulfilling wide scope of necessities.

3) Stop speculating limit Resources don't need to be evaluated before utilization or usage. The assets can be included according to prerequisites.

4) Increase speed and deftness The asset obtaining is simpler and quick. This advances quicker improvement and organization.

5) Stop burning through cash on running and keeping up server farms Maintenance of servers and different assets altogether drops in this sort of framework

6) Go worldwide in minutes Easily send your application in numerous locales around the globe with only a couple of snaps.

A. Types of Cloud Computing

With clout computing the IT departments and developers are being enabled to focus on more important matters like procurement, maintenance and capacity planning rather than having to work on actual hardware implementation. With the growth in popularity of cloud computing, new strategies and models can be developed to match the requirements of different set of users with different levels of control facilitat- ing flexibility. Infrastructures, platforms or softwares can be treated as services. Further understanding is elaborated below. Cloud computing is providing developers and IT depart- ments with the ability to focus on what matters most and avoid undifferentiated work like procurement, maintenance, and capacity planning. As cloud computing has grown in popularity, several different models and deployment strategies have emerged to help meet specific needs of different users. Each type of cloud service, and deployment method, provides you with different levels of control, flexibility, and manage- ment. Understanding the differences between Infrastructure as a Service, Platform as a

Service, and Software as a Service, as well as what deployment strategies you can use, can help you decide what set of services is right for your needs.

1)Infrastructure as a Service (IaaS):

Infrastructure as a Service, sometimes abbreviated as IaaS, contains thebasic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastruc- ture as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today. [7]

2) Platform as a Service (PaaS) :

Stages as an administration expel the requirement for associations to deal with the un-derlying framework (normally equipment and working frameworks) and enable you to concentrate on the organization and the board of your applications. This encourages you be progressively proficient as you dont need to stress over asset scope quantification, programming upkeep, fixing, or any of the other undifferentiated hard work engaged with running your application. [6]

2) Software as a Service (SaaS):

Programming as a Service gives you a finished item that is run and overseen by the specialist co-op. As a rule, individuals alluding to Software as a Service are alluding to end-client applications. With a SaaS offering you don't need to consider how the administration is kept up or how the hidden framework is overseen; you just need to consider how you will utilize that specific piece programming. A typical case of a SaaS application is online email where you can send and get email without overseeing highlight augmentations to the email item or keeping up the servers and working frameworks that the email program is running on. [8]

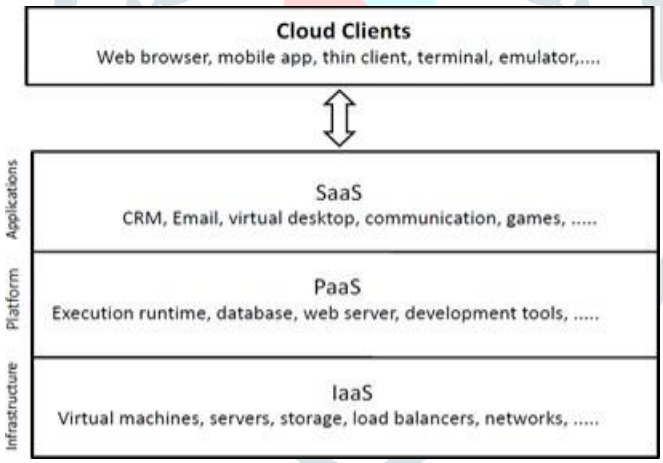

Fig. 1. Cloud Service Platform

B. Implementation Requirements

In present day world the utilization of where the utilization of the distributed storage frameworks and figuring has expanded, all things considered, some basic issues have begun to raise heads. Security of individual information being critical to any framework architect can without much of a stretch be hacked into utilizing the escape clauses in the current frameworks. One such provisos is the sharing of information over the cloud condition. It regularly happens that a client needs to get to some piece of different clients cloud space. Current frameworks permit this entrance by giving the verification information to the mentioning terminal. Despite the fact that this is being finished with the source proprietors assent, this strategy isn't completely protected. At the point when a client shares verification data, the to move unreservedly and hamper the information in the cloud space. A brought together Key Distribution Center utilized does not help in this circumstance since the encryption key can be provided to the two finishes and will be normal. At the point when a client shares validation data, the to move unreservedly and hamper the information in the cloud space. A brought together Key Distribution Center utilized does not help in this circumstance since the encryption key can be provided to both closes and will be normal. Be that as it may if the Key Distribution Center is appropriated to a few nearby key merchants, the encryption of information by one

client cannot be unscrambled by other since the keys will be extraordinary. This is the fundamental work proposed in this paper. [1] There are three cases for privacy issues:

- Case 1: Provider and consumer want to access each other data eld and cloud server inform and shared author- of them. [2]
- Case 2: Consumer want specic data of provider then he request for only that data and other data get protected. [3]
- Case 3: If consumer wants main providers data then it is depend on main provider whether to share or not that data eld. Main provider data eld are not public. [4]

II. Literature Review

In the wake of checking on different papers which proposed different methodologies about information sharing security and keeping up protection of information, following exploration endings has been proposed. The rst paper Secured Multikeyword Ranked Search over encoded cloud information fundamentally center around utilizing multikeyword for seeking information in scrambled structure. Next two papers Privacy saving information imparting to unknown ID task and Providing Privacy Preserving in distributed computing are for the most part center around giving protection to information. Next paper Efcient and secure multikeyword seek on scrambled cloud information proposed Secured positioned catchphrase scan for distributed computing condition. The paper Privacy saving watchword looks on remote encoded information portrays a framework in which Main target is that to give to security and protection by utilizing some encryption technique to remotely put away utilized information. What's more, the last paper Enabling efcient Fuzzy catchphrase look over encoded information in distributed computing proposed Fuzzy watchword pursuit and watchword security is proposed in this framework. The table given beneath demonstrates the writing study for cloud information security procedures.

.

Sr. No.	Paper Title	Objectives
1	Secured Multi-keyword Ranked Search over encrypted cloud data	This paper focus on searching of data in encrypted by using multiple keywords.
2	Privacy preserving data shar- ing with anonymous ID as- signment.	Anonymous ID is given to the user to maintain, privacy ac- cording to this paper.
3	Efcient and secure multi- keyword search on encrypted cloud data.	Secured ranked keyword search for cloud computing environment is proposed in this paper
4	Providing Privacy Preserving in cloud computing	This paper has main objective that it provide individual pri- vacy to each user and some privacy preserving technology use in this paper.
5	Privacy preserving keyword searches on remote encrypted data.	Main objective is that to provide to security and privacy by using some encryption method to remotely stored used data
6	Enabling efcient Fuzzy key- word search over encrypted data in cloud computing.	Fuzzy keyword search and keyword privacy is proposed in this system.

III. RELATED WORK

As we as a whole realize cloud is utilized to store information and offer it among the clients of cloud. Cloud clients might be at remote areas. Cloud Systems has diverse situations. Those conditions are: closes and will be normal. Be that as it may if the Key Distribution Center is dispersed to a few neighborhood key wholesalers, the encryption of information by one client cannot be decoded by other since the keys will be unique. This is the principle work proposed in this paper.:

- Community Cloud: various associations having comparative cloud administrations when in coordinated effort can be known as a network. The people group cloud is simply the cloud this network actualizes or through an outsider association.
- Distributed Cloud When a cloud is implemented with computers spread in different locations, it is called as the distributed cloud. There are two variations in distributed clouds:
  a. Volunteer Cloud
  b. Public-resource Computing
- Inter Cloud Inter cloud is similar to the internet concept. While in internet various networks are connected to each other as a network of many networks, inter cloud is nothing but a connection between various clouds.
- Multi-Cloud Multicloud is the cloud that is implemented by various service providers as viewed from the customer node. This is generally done to tackle the situations of catastrophe where a single service provider is not being able to deliver resources and services.

In past cloud frameworks information get imparted to various diverse clients. However, that information get gotten to by that client which is confirmed or enrolled client. Be that as it may, there is no arrangement of encryption and decoding methodologies. Encryption and decryp-tion is principally use for give security to information while sharing. Past framework did not have those methodologies so it is huge hazard if any information get misfortune by any reason, for example, if any undesirable client gets some significant or private information from association or information get spilled while exchanging from proprietor to client at that point there is opportunities to abuse of that information. It is the huge issue seen in customary cloud framework. We proposed a framework in which information get safely trans-ferred from information proprietor to information client. In this new framework at the client end, client of cloud must be approved. At the point when any client needs any sort of information from any information proprietor rst that client needs to login with his/her ID and secret word. At that point client needs to send solicitation to information proprietor for with respect to information. Presently at the information proprietors end, information put away by the proprietor must be in scrambled structure. Because of this encryption on the off chance that information get misfortune, at that point that information can't utilized by any individual until he/she dont have key to decode it. Presently when approved client sends a solicitation to information proprietor about interest of information requires for him, at that point if information proprietor need to impart that information to client he offers consent to client alongside a key which use to decode information at clients end. At that point client gets encoded information from cloud specialist co-op and in the wake of understanding that information client unscramble it at its end and uses it. Second enormous issue face in past framework that there is no protection for put away information at cloud. In this framework approved client request a few information from information proprietor and on the off chance that he/she get consent from proprietor he/she get to that information which in not in scrambled structure. Think about a worker from any association, he send a solicitation to utilize information and get consent for same. That information was put away in a le where diverse distinctive kind of information gets put away by proprietor. Be that as it may, that representative has authorization to get to information from that le so now he/she can get to another information which might be touchy, at that point there will be opportunities to abuse that information. This condition happens because of absence of access dependent on ciphertext-arrangement characteristic. By utilizing this client can dependably get to its very own information eld as it were. Presently for this issue we utilize triple DES calculation which is lopsided calculation for open key cryptography. In proposed framework on the off chance that client needs to get to information of proprietor, at that point he/she send a solicitation to information proprietor get authorization. On the off chance that proprietor need, at that point he offers consent to the client alongside a key. At that point client utilize that key to get to information from distributed storage, however at this point just that information get gotten to by the client which will coordinate with that key given by the proprietor. In the wake of understanding that information client can decode it and use it. So favorable position of our proposed framework is that private information or information which don't require for client won't access by any client, client can utilize just that information which is allowed by information proprietor. So there will be no loss of private information and abuse of information.

IV. SYSTEM ARCHITECTURE

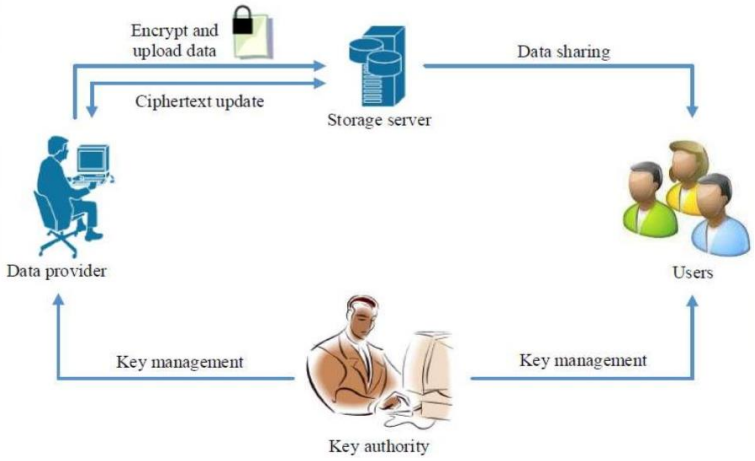

Fig. 2. Cloud Service Proposed System Architecture

1) Revocable Identity Based Encryption is a system that empower a sender to affix the present timeframe to the ciphertext with the end goal that the recipient can unscramble the ciphertext just under the condition that she/he isn't denied at that timespan.
2) In this framework an implosion system is included which demolishes the key of unscrambling after a particular access time of a client is finished. So after that client can not decode the information.

3) Framework Construction Module The information supplier (for example Administrator) choose which client can get to information. The administrator encode information under personality of client and transfer ciphertext of shared information to cloud server.

4) Information Provider Module Data supplier module is a component in which new client can join at first and then login. Information supplier module give alternative of transferring the document to the cloud server utilizing Identity Based Encryption. This module give highlight of implosion and ciphertext update of the record.

5) Key Authority Module Auditor will lognin on the evaluators page and check pending solicitation of any client. In the wake of tolerating demand from the client, He/She will create ace key for encryption and mystery key for unscrambling.

V. ALGORITHM

User first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length 356 = 168 bits. The encryption scheme is illustrated as follows
The encryption-decryption process is as follows :

1. Encrypt the plaintext blocks using single DES with key K1.

2. Now decrypt the output of step 1 using single DES with key K2.

3. Finally, encrypt the output of step 2 using single DES with key K3.

4. The output of step 3 is the ciphertext.

5. Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.

6. Due to this design of Triple DES as an encryptdecrypten- crypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K1, K2, and K3 to be the same value. This provides backwards compatibility with DES.

7. Second variant of Triple DES (2TDES) is identical to 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and finally encrypt with K1 again. There- fore, 2TDES has a key length of 112 bits.

8. Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES.

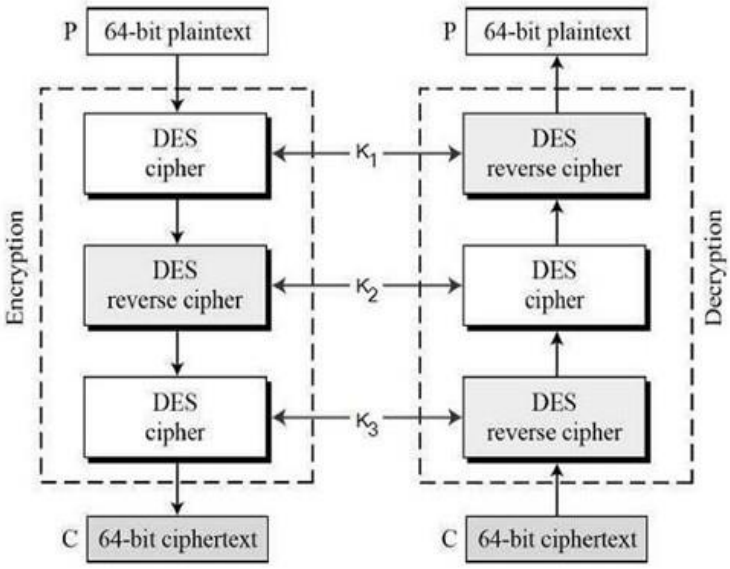

Fig. 3. Encryption Scheme

VI. MATHMATICAL MODEL

User = a	Request = r	Encryption = E
Decryption = D	User ID of User a = UID a	User ID of User b = UID b
Data = x	Admin = w	Time To Live = t

1. User a Send Request For Data x to Admin
   w = r [(a (x))]

2. Admin grant request from a & Encrypt data using identity of ser having time to live t
   E [(UID a (x (t))]

3. Secret key is shared with user decrypt the data
   D [(UID a (x (t))]

4. User get data if following condition get satisfied
   E [(UID a (x (t))] = D [(UID a (x (t))]

5. After Time To Live or user authorization is over then Data Provider Module update the ciphertext i.e.,
   E [(UID a (x (t))]

6. Now the data get re-encrypted and ciphertext is E(x)
   E(x) doesn't match with D [(UID a (x (t))] so user a can not access data x.

VII. CONCLUSION

The aim towards recognizing the risks involved in data sharing in the cloud environment enables the improvements in data security,data integrity,data anonymity and user privacy. We have also proposed a system improvement for the same. The proposed system is expected to improve security levels further in cloud computing and storage.

REFERENCES

[1]Hong Liu, Huansheng Ning, Qingxu Xiong, and Laurence T. Yang,Shared Authority Based Privacy-preserving Authentication Proto- col in Cloud Computing,IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL:PP NO:99 YEAR 2014.

[2]H. Takabi, J.B.D. Joshi, and G. Ahn,-Security and Privacy Challenges in Cloud Computing Environments, IEEE Security & Privacy, vol. 8, no. 6, pp. 24-31, NDec. 2010.
[3]M. Armbrust, A. Fox, R. Grifth, A.D. Joseph, R. Katz, A. Konwinski,
G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, -A View of Cloud Computing, Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010.H.
[4]C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy- preserving public auditing for data storage security in cloud computing, in INFOCOM, 2010 Proceedings IEEE, march 2010, pp. 1-9.
[5]R. Laurikainen, Secure and anonymous communication in the cloud, Aalto University School of Science and Technology, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10, 2010.
[6]M. Jensen, S. Schage, and J. Schwenk, Towards an anonymous access control and accountability scheme for cloud computing, in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, July 2010, pp. 540-541.
[7]L. Malina and M. Zukal, Secure authentication and key establishment in the sip architecture, in Telecommunications and Signal Processing(TSP), 2011 34th International Conference on. IEEE, 2011, pp. 1418.
[8] Wang, B.; Baochun; Wang, H. L. 2012 Oruta:Privacy- Preserving Public Auditing for Shared Data in the Cloud, IEEE Fifth International Confer- ence on Cloud Computing, 2012 IEEE, DOI 10.1109CLOUD.2012.46.
[9]W, Jian; Y, Wang; J, Shuo and Le,Jiajin; Providing Privacy Preserving in cloud computing, 2009 International Conference on Test and Mea- surement, 2009 IEEE, ICTM 2009.
[10]D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano ,Public Key Encrption with Keyword Search In proceedings of Eurocrypt 2004, LNCS 3027, pp. 506-522, 2004.
[11]Yong Ho Hwang and Pil Joong Lee, -Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System,Lecture Notes in Computer Science, 2007, Volume 4575/2007, 2-22 [12]Changyu Dong, Giovanni Russello and Naranker Dulay ,Sharable and Searchable Encrypted Data for Untrusted Servers, Proceeedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applica- tions Security pp 127-143.
[13]Liu Hong-xia, -Research on privacy preserving keyword search in cloud storage ,Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on 9-11 July 2010 ,pp 444 446.
[14]Shuhui Hou ,Secure and Privacy Preserving keyword search for cloud storage devices, Multimedia Information Networking and Security (MINES), 2011 Third International Conference on 4-6 Nov. 2011,pp 595 599.
[15]Shucheng Yu, Kui Ren ,Wenjing Lou - Achieving Secure ,Scalable and ne grained data access control in cloud computing Proceeding INFOCOM10 Proceedings of the 29th conference on Information com- munications Pages 534-542.
[16]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus- scalable secure le sharing on untrusted storage. In Proceedings of the Second USENIX Conference on File and Storage Technologies(FAST). USENIX, March 2003.
[17]Ankatha Samuyelu Raja Vasanthi ,Secured Multi keyword Ranked Search over Encrypted Cloud Data, 2012.
[18]S. Pearson, Y. Shen, and M. Mowbray, A privacy manager for cloud computing in Cloud Computing. Springer Berlin/ Heidelberg, 2009, pp. 90-106.
[19]M. Mowbray, S. Pearson, and Y. Shen, Enhancing privacy in cloud computing via policy-based obfuscation. Springer Berlin / Heidelberg, 2010, pp. 1-25.
[20]C. Ardagna, S. De Capitani di Vimercati, S. Paraboschi, E. Pedrini, and P. Samarati, An XACML-based privacy centered access control system, in Proceedings of the rst ACM workshop on Information security governance. NewYork, NY, USA: ACM, 2009, pp. 49-58.
[21]J.Li, Q.Wang, C.Wang, N.Cao, K.Ren, and W.Lou, Fuzzy keyword search over encrypted data in cloud computing, in Proc. of IEEE INFOCOM10 Mini-Conference, San Diego, CA, USA, March 2010.
[22]J.Li, Q.Wang, C.Wang, N.Cao, K.Ren, and W.Lou, Fuzzy keyword search over encrypted data in cloud computing, in Proc. of IEEE INFOCOM10 Mini-Conference, San Diego, CA, USA, March 2010.
[23]A.Lewko, T.Okamoto, A.Sahai, K.Takashima, and B.Waters, Fully se- cure functional encryption: Attribute- based encryption and (hierarchi- cal) inner product encryption, in Proc. of EUROCRYPT, 2010.