iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** I **Month of publication:** January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1415

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 :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Preserving Data Confidentiality in Cloud Computing

Mr. A.R. Gadekar[1], Dr. M.V. Sarode[2], Dr. V.M. Thakare[3]
[1, 2, 3]*Department of Computer Science & Engineering, SGBA University*

Abstract*: Utilizing an indistinguishable key for both encryption and decryption is the key standard in symmetric algorithm. This component includes the presence of brought together Key Distribution Center otherwise called KDC, in charge of appropriating and keeping up attributes and secret keys to its clients. There's an additional mechanism for decentralized access control used to make information more secure on cloud. The security in these frameworks endures a noteworthy disadvantage when one client demands for the sharing of information of some other's client. This methodology includes a few escape clauses that can enable the offender to access individual data in the cloud storage.
Index Terms: Symmetric Algorithm , Key Distribution Center, Paillier Algorithm.

I. INTRODUCTION

In the modern world, the use of cloud storage systems and computing has largely grown and some of the key issues have started to pick up. For any system engineer, the security of personal data is important and can easily exploit vulnerabilities in existing systems for attack. One such loophole is to share data in a cloud environment. Often, users need to access part of the cloud space of other users. Current systems allow such access by providing authentication data to the requesting terminal. This process is not completely secure, even with the consent of the source owner. As users share authentication information, they move freely and block data in cloud space. Since the encryption key can be provided to both ends, the centralized key distribution center adopted does not work in this case. As users share authentication information, they move freely and block data in cloud space. A centralized key distribution center does not work in this case because the encryption key can be provided to both ends and is universal. [1] However, if the key distribution center is distributed to multiple local key distributors, one user's data encryption cannot be decrypted by other users because the keys will be different. This is the main work proposed in this paper. There are three privacy issues:

Case 1: Suppliers and consumers want to access each other's data domains and cloud servers to inform and share their power [2].

Case 2: Consumers need vendor-specific data, and then he only asks for data and other data to be protected [3].

Case 3: If the consumer wants the main provider data, then whether the main provider wants to share this data field. The main provider data fields are not public. [4]

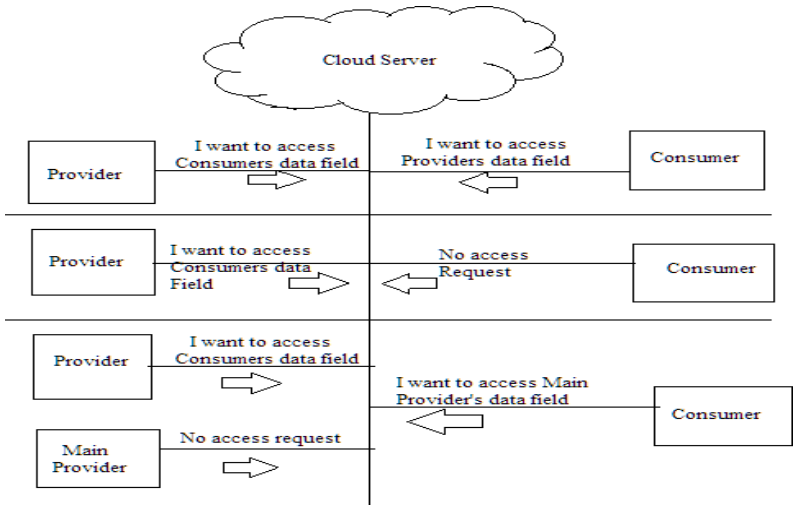


Fig. 1. Three cases of data sharing and accessing

A. There are three types of platform in the cloud:

1) *Cloud clients:* Cloud clients are all devices that use cloud resources for storage or computing. These devices can be cell phones, personal computers, servers and more. Some devices that use cloud computing cannot run without a connection to a server or cloud. The basic requirement for these devices as clients is that they must be connected to the cloud via Ethernet. Depending on the nature of the cloud environment, the server may require special software to run on client nodes. But it can also be done using a web browser installed on the client [5]
2) *Platform as a service cloud (PaaS):* Paas operates by providing service providers with not only resources but also application development and operations platforms. This platform is nothing more than the operating system itself and some applications running on it. Users can develop custom applications in this environment. Service Providers also make rules and languages for application development in this domain. In some advanced PaaS environments, users do not need to manually allocate resources. Resources are automatically allocated on demand and supply[6]
3) *Enterprise PaaS Examples:* Apprenda Common PaaS Use-Case: Increases developer productivity and utilization rates while also decreasing an application's time-to-market

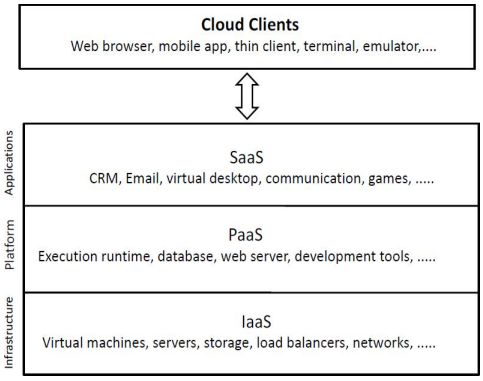


Fig. 2. Cloud Service Platform

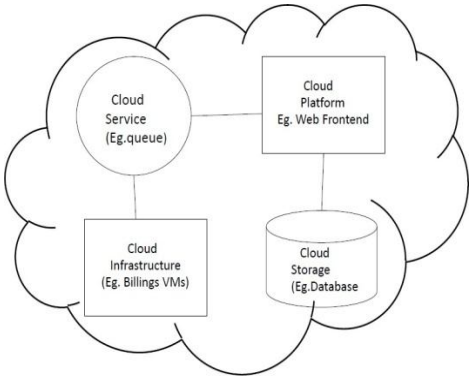


Fig. 3. Cloud Service Platform

4) *Infrastructure as a service cloud (IaaS)*Generally, providers of IaaS offer physical or virtual machines with additional resources. These resources are provided as per demand from a large pool of availability. Customers choose between Carrier cloud or Internet for WAN connectivity. In order to deploy applications, operating systems need to be installed in the cloud environment by the customers. Customers are responsible for operating and maintaining the applications and operating systems in the cloud environment in this system. Billing is done on the basis of how much resources are used by which user.[7]
5) *IaaS Examples:* Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE), J Common IaaS Use-Case: Extends current data center infrastructure for temporary workloads (e.g. increased Christmas holiday site traffic)
6) *Software as a service(SaaS)*Databases and application software's are accessed by the user in SaaS environment. These applications and databases run on virtual computing environment. The service provider is free to distribute the computation among different resources available. The user is able to see this procedure of transfer between machines. It is sometimes known as software on demand. Billing is done according to the pay-per-use basis. Here the server can access applications in client and vice versa.[8]
7) *SaaS Examples:* Google Apps, Sales force, Workday, Concur, Citrix Go To Meeting, Cisco Web
8) *Common SaaS Use-Case:* Replaces traditional on-device software
9) *Cloud system is divided into three types:*
10) *Private cloud:* A cloud infrastructure that is implemented by and is dedicated to a single organization is known as the private cloud. Private clouds when implemented correctly may enhance the business to a great extent. But this has to be done very carefully as each stage in the environment adds to more and more complexity and security issues. These security issues should be tacked correctly which requires skilled professional and quality hardware. This induces greater costs. Thus so far only powerful and wealthy companies are being able to develop such infrastructure. The private cloud no doubt also needs a physical space for hardware placement and management.
11) *Public cloud:* A public cloud is the cloud whose resources are not owned and used by a single organization. The cloud is available for use by different users, hence called as public cloud. The difference between public and private clouds can lie in

security considerations. Public cloud is made available by a single cloud owner or service provider. The users are charged as per usage. The security issues mainly arise in this environment as all the users are using same resources. This makes it crucially important to implement user identification so that no data from one user drops to potentially hazardous location or user.[9]

12) *Hybrid Cloud:* Hybrid cloud is nothing but the functional combination of a public cloud with private cloud. It may happen that a company may need to store critical data in its own private cloud. But sometimes the need may arise to share this data to the public cloud. The implementation required is nothing but a hybrid cloud. In Hybrid cloud, the organizations owning their own private clouds only need to send data to public cloud when additional resources of computing are demanded. The merit of this system is that the customers are billed according to the amount of these resource al locations.[10]

II. LITERATUREREVIEW

After reviewing various papers which proposed various strategies about data sharing security and maintaining privacy of data, following research findings has been proposed. The first paper Secured Multi keyword Ranked Search over encrypted cloud data mainly focus on using multi keyword for searching data in encrypted form. Next two papers Privacy preserving data sharing with anonymous ID assignment and Providing Privacy Preserving in cloud computing are mainly focus on providing privacy to data. Next paper Efficient and secure multi keyword search on encrypted cloud data proposed Secured ranked keyword search for cloud computing environment. The paper Privacy preserving key word searches on remote encrypted data describes a system in which Main objective is that to provide to security and privacy by using some encryption method to remotely stored used data. And the last paper Enabling efficient Fuzzy keyword search over encrypted data in cloud computing proposed Fuzzy keyword search and keyword privacy is proposed in this system. The table given below shows the literature survey for cloud data security strategies.

Table i
Literature survey

Sr no	Paper Title	Objectives
1	Secured Multi-keyword Ranked Search over encrypted cloud data	This paper focus onsearching of data in encrypted by using multiple keywords.
2	Privacy preserving data sharing with anonymous ID assignment.	Anonymous ID is given to the user to maintain privacy according to this paper.
3	Efficient 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 privacy 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 efficient Fuzzy keyword search over encrypted data in cloud computing.	Fuzzy keyword search and keyword privacy is proposed in this system.

III. PROPOSEDWORK

As we all know cloud is used to store data and share it among the users of cloud. Cloud users may be at remote locations. Cloud Systems has different environments. Those environments are:

A. Community Cloud

A number of organizations having similar cloud services when in collaboration can be known as a community. The community cloud is the cloud this community implements itself or through a third-party organization.

B. Distributed Cloud

When a cloud is implemented with computers spread in different locations, it is called asthe distributed cloud. There are two variations in distributed clouds:

1) Volunteer Cloud
2) Public-resource Computing

C. 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.

D. Multi-Cloud

- Multi cloud 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 previous cloud systems data get shared with different- different users. But that data get accessed by that user which is authenticated or registered user. But there is no provision of encryption and decryption strategies. Encryption and decryption is mainly use for provide security for data while sharing. Previous system did not have those strategies so it is big risk if any data get loss by any reason such as if any unwanted user gets some important or private data from organization or data get leaked while transferring from owner to user then there is chances to misuse of that data. It is the big issues potted in traditional cloud system. We proposed a system in which data get securely transferred from data owner to data user. In this new system at the user end, user of cloud must be authorized. When any user wants any kind of data from any data owner first that user has to login with his/her ID and password. Then user has to send request to data owner for regarding data. Now at the data owners end, data stored by the owner must be in encrypted form. Due to this encryption if data get loss then that data cannot used by any person until he/she don't have key to decrypt it. Now when authorized user sends a request to data owner about demand of data requires for him, then if data owner want to share that data with user he gives permission to user along with a key which use to decrypt data at users end. Then user get sencrypted data from cloud service provider and after getting that data user decryptit at it send and uses it. Second big issue face in previous system that there is no privacy for stored data at cloud. In this system authorized user demand some data from data owner and if he/she get permission from owner he/she access that data which in not in encrypted form. Consider an employee from any organization, he send a request to use data and get permission for same. That data was stored in a file where different-different type of data gets stored by owner. But that employee has permission to get access data from that file so now he/she can access another data which may be sensitive, then there will be chances to misuse that data. This condition occurs due to lack of access based on cipher text-policy attribute. By using this user can reliably access its own data field only. Now for this issue we use pailler's algorithm which is asymmetric algorithm for public key cryptography. In proposed system if user wants to access data of owner then he/she send a request to data owner get permission. If owner want then he gives permission to the user along with a key. Then user use that key to access data from cloud storage, but now only that data get accessed by the user which will match with that key given by the owner. After getting that data user can decrypt it and use it. So advantage of our proposed system is that private data or data which do not require for user will not access by any user, user can use only that data which is permitted by data owner. So there will be no loss of private data and misuse of data.

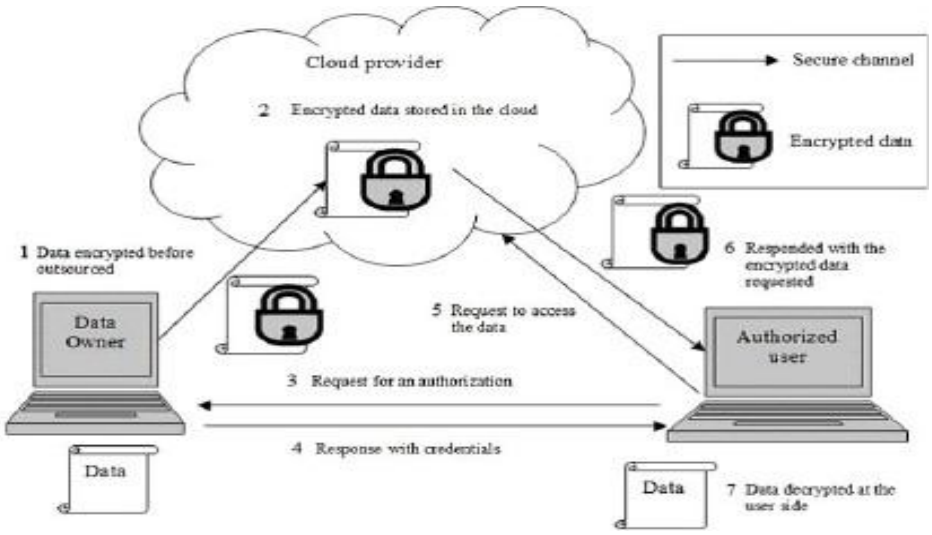


Fig. 4. Proposed System Architecture

IV. SYSTEMARCHITECTURE

A. *Modular Structure*: The system works in the form of different modules having different functions each
B. *Owner Registration*: In order to upload data to a cloud, the user needs to be registered first. Registration refers to saving the data regarding the user in a system database. This is an important stage since the users can not use the cloud anonymously or ambiguously
C. *Owner Login*: This module a registered data owner has to prove his identity every time he has to access the cloud. This phase includes the owner providing his authentication credentials
D. *User Registration*: A like owner registration, each user also needs to provide his/her information to the authentication database in order to register and be able to use the cloud resources
E. *User Login*: This is the stage where the user provides the authentication credentials. These credentials are matched with the registration database entries and the user is identified. This stage helps in holding responsible a user involved in data theft or unauthorized access.
F. *Access Control*: Owner in this system only can allow or deny access to their data for some user in the system. No user has access to the data if the owner does not permit. User may further have the facility to limit this access for a particular time or particular number of times only.[15
G. *Encryption & Decryption*: Uploaded files are encrypted before uploading to the cloud. Similarly while accessing the data, it needs to be decrypted. This encryption and decryption can add to the security to a great extent. The owner can have the right to encrypt data segments with different keys and then provide the users the keys only to which he wants to restrict the access to the user.
H. *File Upload*: File uploading can be done by owner after the encryption module. This file is saved in a remote database and can be downloaded by a registered and authorized user only. During download, the data can be decrypted only with the key it was encrypted with
I. *File Download*: Once authorized the user can download and decrypt the required data. The decryption key needs to be provided by the owner
J. *Cloud Service Provider Registration*: Like user and owner, cloud manager also has to register in a similar way. Cloud service provider or manager is the person that can access all the data on cloud. This entity is like a trustee and needs to be trusted by user and owner
K. *Cloud Service Provider Login*: After login, could service provider can have access to all the data on cloud. He does not need authorization.
L. *TTP (Trusted Third Party) Login*: A trusted third party or TTP is a person that is not in any of the above roles but is trusted as a monitor against malpractices with the uploaded data. They do not upload or access any data available on cloud.[16]

V. ALGORITHM

A. *Creation ofKDC*

To create a different number of KDC's given a input as KDC name, KDC id and KDC password it will save in a database and to register a user details given an input as user name and user-id.[17]

B. *Paillier Algorithm*

There are various homomorphic encryption methods. But the most efficient is Pailiers algorithm. Base of this system is Decisional composite residuosity assumption: Consider

Given N = pq,

If k is the security parameter. Two k-bit primes p and q are chosen uniformly at random $N = pq$. To encrypt a message $m < N$, one chooses a random value r belong to $Z * n$. and computes the cipher text as:

$c = g^m r^m mod N^2$

When receiving a cipher text c, it is checked whether that $c < N^2$, if yes then message m is receive as

$$m = L(c^{\lambda(N)} mod N^2) \quad (1)$$
$$L(g^{\lambda(N)} mod N^2) mod N$$

C. *Properties*

1) Multiplication of encrypted messages result in addition of given plain-text.

$D[E(m_1) * E(m_2) mod n^2] = m_1 + m_2 mod n$

Raising of cipher text to constant power result in constant multiple of givenplain-text.

$D[E(m)^k mod n^2]= k*mmodn$

D. Encryption

Let *m*be a message to be encrypted where m^{Zn}. Select random *r* where$rZ_* n$. Compute cipher text as:

$c=gm.r^n mod n^2$.

E. Decryption

Cipher text: c^Z n^2.Compute message: $m = L(c\lambda mod n^2).modn$.[21]

VI.MATHEMATICAL MODEL

$U = U_1, U_2, U_3, ...,U_n, n>0$

$= \sum_{i=1}^{n} Ui$

U is a set of users.

$P = P_1, P_2, P_3, ...,P_n, n>0$

$= \sum_{i=1}^{n} Pi$

P is set of access permissions.

$P = U_1P_1, U_1P_2, U_1P_3, ..., U_1P_n, n >0$

$$= \sum_{i=1}^{n} Ui\ Pi$$

UP is set of users access permissions.

$$\sum_{i=1}^{n} rUiPi = \sum_{i=0}^{n} Pi + \sum_{i=0}^{n} UiPi$$

where,

rU_iP_i-set of al located access permission to users,

P_i-set of users own permission,

U_iP_i-set of other access permission as sign to user

TABLE II

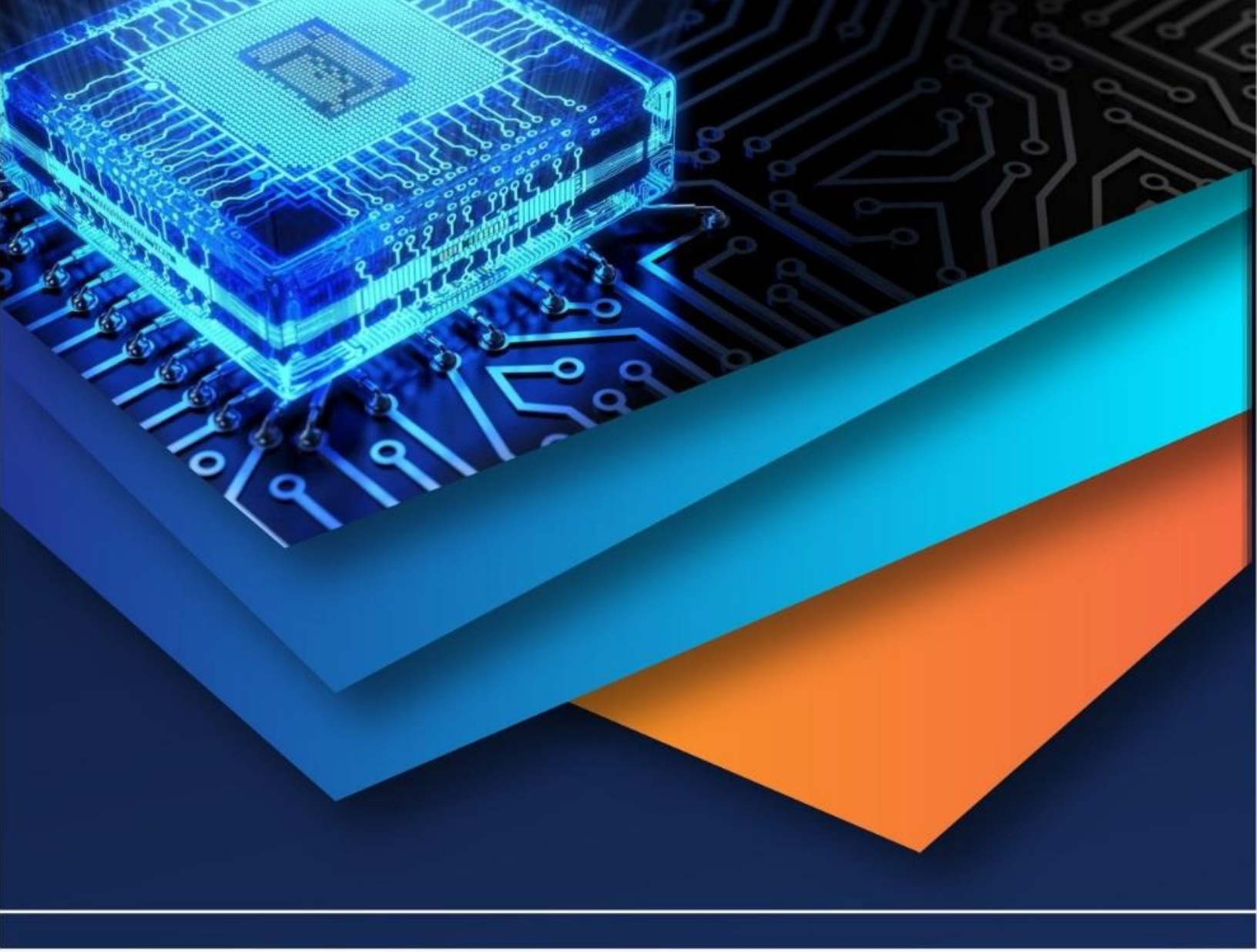
USER1	USER2
STEP 1	
Choose a number A, Keep it secret.A=3	Choose a number B, Keep it secret. B=6
STEP 2	
puts 5 through 7A (mod 11) 73 (mod11) = 343 (mod 11) = 2	puts 6 through 7B (mod 11) 76 (mod11) = 117649 (mod 11) = 4
STEP 3	
calls result α Send 2 to user 2	calls result β Send 4 to user 1
STEP 4	
puts β through βˆA(mod11) 43(mod11) = 64(mod11) = 9	puts α through αB (mod11) 26 (mod11) = 64(mod11) = 9.[22]

VII. CONCLUSION

The aim towards recognizing the risks involved in data sharing in the cloud environment enables the improvements in data security, data in tegrity, 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, HuanshengNing, QingxuXiong, and LaurenceT.Yang,"SharedAuthorityBasedPrivacy-preservingAuthentication Protocol 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.Griffith,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,"Secureandanonymouscommunicationin thecloud",AaltoUniversitySchoolofScienceandTechnology, Department of Computer Science and Engineering, Tech. Rep. TKK-CSE-B10,2010.
[6] M. Jensen, S. Schage, and J. Schwenk, "Towards an anonymousaccesscontrolandaccountabilityschemeforcloud 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 Conferenceon.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 Conference on Cloud Computing, 2012 IEEE, DOI10.1109CLOUD.2012.46.
[9] W, Jian; Y, Wang; J, Shuo and Le,Jiajin; "Providing Privacy Preserving in cloud computing", 2009 International Conference on Test and Measurement, 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 PilJoong 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 NarankerDulay"Sharable and Searchable Encrypted Data for Untrusted Servers", Proceeedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applications 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 InternationalConferenceon9-11July2010,pp444446.
[14] ShuhuiHou ,"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,pp595 599.
[15] ShuchengYu, KuiRen- Achieving Secure ,"Scalable and fine grained data access control in cloud computing" Proceeding INFOCOM'10 Proceedings of the 29th conference on Information communications Pages 534-542.
[16] M. Kallahalla, E. Riedel, R. Swaminathan, and K. Fu. Plutus-"scalable secure file sharing on untrusted storage". In Proceedings of the Second USENIXConference on File and Storage Technologies(FAST). USENIX, March 2003.
[17] AnkathaSamuyelu Raja Vasanthi,"Secured Multi keywordRankedSearchoverEncryptedCloudData",2012
[18] S. Pearson, Y.Shen, and M. Mowbray, "A privacy manager for cloud computing in Cloud Computing". Springer Mowbray, S. Pearson, and Y.Shen, "Enhancing privacy in cloud computing via policy-based obfuscation." SpringerBerlin/Heidelberg,2010,pp.1-25.
[19] C.Ardagna,S.DeCapitanidiVimercati,S.Paraboschi,E. Pedrini, and P. Samarati, "An XACML-based privacy centered access control system," in Proceedings of the first ACM workshop
[20] 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, SanDiego,CA,USA,March2010.
[21] R.Brinkman, "Searching in encrypted data," in University of Twente, PhDthesis,2007.
[22] A.Lewko, T.Okamoto, A.Sahai, K.Takashima, and B.Waters, "Fully secure functional encryption: Attribute- based encryption and (hierarchical) inner product encryption," in Proc. of EUROCRYPT,2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY