International Journal of Engineering & Technology, 7 (4.6) (2018) 481-486

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Efficient Securing Data using Enhanced Key Policy Attribute based Encryption in Cloud

M.Saraswathi[1]*, T.Bhuvaneswari[2]

[1] *Assistant Professor, Department of CSE SCSVMV University, Enathur,Kanchipuram, Tamilnadu*
[2]*Assistant Professor,Department of Computer Applications,Queen's Mary College, ChennaiTamilnadu,*
**Corresponding author E-mail: [1]saraswathi.kumar@gmail.com*

Abstract

With the tremendous growth of sensitive records on cloud, cloud security is getting more necessary than even before. The cloud data and offerings reside in hugely scalable statistics centers and can be accessed everywhere. The increase of the cloud customers been accompanied with a growth in malicious undertaking in the cloud. More and more vulnerabilities are discovered, and nearly every day new security advisories are published .In this regard to protect data from leaking, users need to encrypt the data before outsourcing. The Cloud service provider (CSP) should ensure integrity, availability, privacy and confidentiality of user data. The objective of this paper aims to provide a solution that ensures the storage of data securely in the cloud. A Proposed an algorithm as enhanced-key policy attribute-based encryption scheme (KP-ABE) for data security in cloud storage .Data owners encrypt their secret data for the data receivers using enhanced KP-ABE algorithm. By applying proposed algorithm overall key generation, Encryption and decryption time is minimized.

Keywords: *Cloudsecurity, Integrity, availability, privacy, Encryption, Decryption.*

1. Introduction

Cloud computing is a paradigm shift from traditional computing that relies on sharing of computer resources rather than having personal devices. Cloud computing provides flexible and cost effective way to access the data to end users in multiplatform at any time. The sharing of resources includes storage, software and hardware[1]. The cloud offers different administrations like SaaS, PaaS, IaaS, MaaS, SecaaS2 .The fundamental idea driving the cloud is Virtualization. The secrecy, openness, security, protection, execution, uprightness are the significant issue of cloud .The cloud gives distinctive sorts of cloud organization models like public, private, hybrid and community cloud network. Cloud computing is a developing innovation as the quantity of cloud specialist organizations and the cloud clients are expanded as of late. The income of cloud computing in 2009 is around 58 billion US dollars. In 2010, 70 billion US dollars. The income increment is around 16-17 contrasted with a year ago. The present day cloud application managed customer and independent venture needs as opposed to mission basic or huge business application. Effect of security breaks for extensive scale business and mission basic application will be significantly high contrasted with little scale business. The income produced by the cloud computing relies on the Nature of Administration offered by the cloud specialist. The essential trait of Nature of Administration is security and the cloud specialist needs to give full affirmation of security as far as classification, openness, protection and honesty. Among the elements protection is an essential and uncompromisable factor of security. Encryption is the best approach to secure the information in the untrusted cloud server. The majority of Encryption methods of Encryption strategies right now accessible had no impact on constant cloud applications. The possibility of their use in critical cloud application is limited. Thus we classify different encryption algorithms based on their usability and adaptability using Attribute Based Encryption (ABE). Unlike other encryption methods the ABE dealt with encrypting and decrypting the data based on user attributes. It gives promising and adaptable access control by utilizing controlled access structures related with private key, access key and the cipher text.

2. Related Work

Kaitai Liang [5] et al propose the first cloud-based revocable identity-based proxy re-encryption (CR-IB-PRE) scheme supports client revocation but also allocation of decryption permissions. At the end of a given time period the cloud acting as a proxy will re-encrypt all cipher text of the user under the current time period to the next time period. If the end user is revoked in the forthcoming time period, he/she unable to decrypt the cipher texts by using the expired private key. Using this approach Communication and computation efficiency is increased but it can be applicable in Constant size cipher text only.

Youngho park [6] et al present a fully secure CP-ABE system with non-monotonic access structure for large attribute space. Our system achieves fully secure definition by giving a proof that any polynomi-

al time attacker cannot distinguish the distribution in a real game and a final game by using dual encryption framework. This mean the challenger can-not make decryption to the challenge ciphertext with queried secret key include those that satisfy the challenge access structure. Moreover, our scheme also allows user to define NOT gates in the access tree besides AND, OR and threshold gates which add the ex-press ability of access control. Our present CP-ABE system also allows large attribute universe since the public parameter in the present CP-ABE does not grow linearly with attribute space size. Furthermore, from analysis of memory requirement and computation cost, our proposed CP-ABE is feasible to be used in real application.

Y.Yang [7] presented an extended proxy-assisted approach in order to overcome the limitation of needing to trust the cloud server not to disclose users' proxy keys inherent in proxy/mediator assisted user revocation approaches. In this approach, bind the cloud server's private key to the data decryption operation, which requires the cloud server to reveal its private key should the cloud server decide to collude with revoked users. We then formulated a primitive, 'revocable cloud data encryption', under the approach. The experimental results suggested that this approach is suitable on smart mobile devices.

Ming Li et al. [8] displayed a contextual analysis utilizing online Personal Health Record (PHR), they first demonstrate the need of pursuit ability approval that says the Authorized Private Keyword Search (APKS) over scrambled cloud information. They then propose two novel answers for APKS in light of a late cryptographic primitive, Hierarchical Predicate Encryption (HPE). Their answers empower proficient multi-dimensional catchphrase seeks with reach inquiry; permit designation and renouncement of pursuit abilities.

Yanjiang Yang et al. [12] propose that Storage-as-an administration is a crucial part of the distributed computing framework. Database outsourcing is a run of the refine use situation of the distributed storage administrations, wherein data encryption is a decent approach empowering the information proprietor to hold its control over the outsourced information. Searchable encryption is a cryptographic primitive taking into consideration private watchword based pursuit over the scrambled database. The setting of big business outsourcing database to the cloud requires multiclient searchable encryption, while for all intents and purposes every single existing plan consider the single-client setting.

Joseph K. Liu et al [14] presented another fine-grained Two Factor Authentication (2FA) control framework. Particularly, in this 2FA control technique, attribute-based access technique isexecuted with the requirement of both user secrecy key and security device. It is not possible to access and hold by user. Also this method is really used to improve the security mechanism. Generally these methods are available in cloud web service. Additionally, attribution based methods provide user privacy from others.

3. Issues In Cloud Computing

Cloud security is the most important issue like multi tenancy, data loss ,data leakage, easy data access cloud, identity management, Key management, Availability Data Integrity , Data Confidentiality ,unsafe API's, service level agreement inconsistencies, patch management, internal threats etc.Cyber crime's effects are felt throughout the Internet, and cloud computing is an enticing target for many reasons. Cloud Providers such as Google, Microsoft, and Amazon have the exciting infrastructure to deflect and survive cyber-attacks, but not every cloud has such capability. It is not easy to enforce all the security measures that meet the security needs of all the users, because different users may have different security demands based upon their objective of using the cloud services.

4. Problem Statement

To successfully address above cloud security issues, we need to understand the compound security. Challenges in a holistic way. Specifically, we need to: (i) investigate various cloud security attributes including vulnerabilities, threats, risks, and attack models; (ii) identify the security requirements including confidentiality, integrity, availability, transparency, *etc*.; (iii) identify the involved parties (clients, service provides, outsiders, insiders) and the role of each party in the attack-defense cycle; (iv) understand the impact of security on various cloud deployment models (public, community, private, hybrid). Storing Data in cloud is most significant of any real system or organization. The information are originating from cloud utilizing open system (web) there are opportunities to hack the information. There have been groupof work done on security problem and difficulties yet at the same time there isn't 100% full confirmation solution. There are numerous physical and some other attack on information that destroy information on server. One solution for this problem is distributed the information to more than one server rather than one server and data will stored in encrypted format using high secure algorithm.

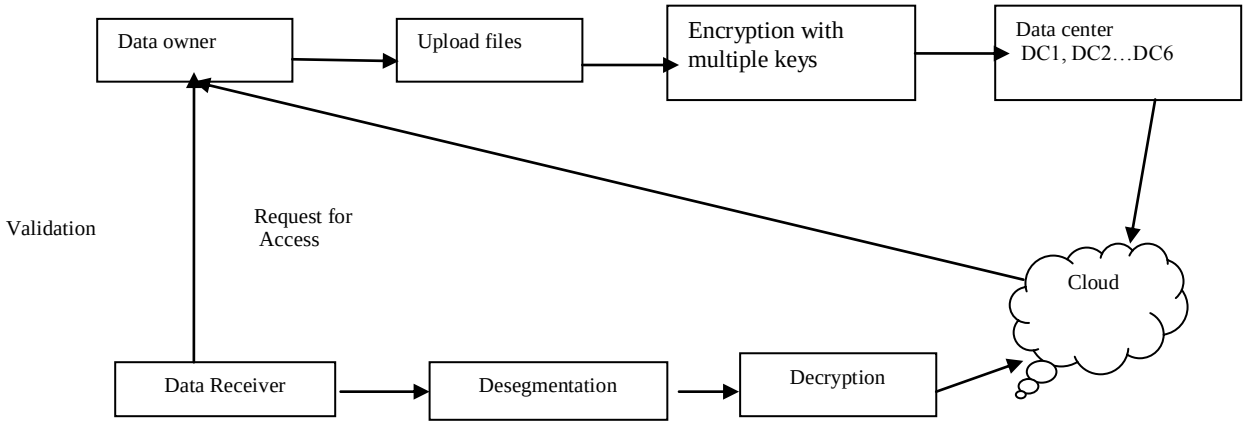
5. Problem Solution

In cloud computing security is a critical part of nature of administration.Encryption is a better solution to secure information in cloud environment. The main contribution of this paper is that, a secure encryption scheme to share encrypted data among a set of authorized users and to achieve efficient user revocation for clouds.

Several encryption techniques are used to keep the sensitive user data confidential against untrusted servers. KP-ABE (Key-Policy Attribute based encryption) encryption scheme based on the trusted authority has been proposed that leverages the performance required for encryption tasks inside the cloud itself. A trusted authority is only responsible for key re-generation, resulting in a more efficient and scalable security.

We propose a cloud-based secure data system, which allows trusted authority to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of data receiver. Using this technique overall reduce the key management complexity of authority owners and data receivers. Differentiation from previous cloud-based data system, Data owners encrypts their secret data for the data receivers using Enhanced **KP-ABE Encryption scheme**. After the encryption process the data split into six parts and stored in a different division in the cloud (data centers).

Another advanced feature is, if any data receiver wants to download a file, the data receiver will send the request to the authority (data owner).With data owner permission only able to access data. If the Owner wants to share the original file with the data receiver, he accepts the request otherwise data owner decline the request. After accepts request the data receiver download the keys and this key's are mainly for validation and to download the data in the original format (decrypted format).



6. System Model

1. Data Owner Setup: Each Owner D_i generates user's secret and public key pair
kG *(1l) (Sk$_i$; Pk$_i$)* and an access structure *D$_i$*, here i=1, 2; . . .N.

2. Encryption: a message (m) and a set of attributes (*DC)*, and outputs the cipher text CT, whereas
Dc= {Dc$_1$, Dc$_2$.....Dc$_N$} ˜Dc$_i$ ∩ D$_i$.

3. Segmentation:, a message M and a set of attributes *DC*, and outputs the cipher text CT in to 6 parts DC_1, DC_2…..DC_6, where *Dc={ Dc$_1$,Dc$_2$.....DcN} ˜Dc$_i$ ∩ Di*

4. Keygen:

Each Owner Di takes as input user's secret key Sk_i, a global identifier GID and a set of attributes *Di* GID, and outputs the secret keys *Sk$_i$U*, where *D$_i$GID = DGID ∩D$_i$, DGID* and *D$_i$*denote the attributes corresponding to the GID and monitored by D_i, respectively.

5. Desegmentation: This algorithm includes following inputs such as Pk_i, Sk_i and verifies where *DC={ DC$_1$, DC$_2$.....DC$_N$} ˜DC$_i$ ∩ D$_i$* DC_1, DC_2…..DC_6 to message M.

6. Decryption: This algorithm takes as input as a GID the secret keys cipher text (CT) and outputs the message is denoted as M
Steps of algorithm

Step I: Initialization
1: Methodology Instatement ( )
2: Instate figure file classes with its record estimate
3: Create open key by utilizing rundown of figure record class and properties, produce irregular list
4: Create other key by utilizing rundown of figure list class and characteristics, produce arbitrary list
5: for each i=0 where i<bytes1.length
6: String j= figure record class name + irregular (I);
7: String str= Integer.toBinaryString (j)
8: increase I;
9: end for
10: end Technique

Step II: Encryption of file
1: Strategy Encryption (b)
2: key instatement
3: Accepts entire record as msg
4: FOS=new FileoutputStream (out)
5: byte [] b=new byte [8];
6: int I-cis.read (b);
7: while I! = - 1 complete
8: fos.write (b, 0, I);
9: i=cis.read (b);
10: end while
11: end Method 37

Step III: Key generation
1: Technique Summation Keygen ( )
2: Veiling open key and byte organize
3: Veiling insurance key and byte design
4: for each i=0 upto i<byptes12.lenght
5: int j=bytes12 [i];
6: String s3=Integer.toBinaryString (j);
7: String temp= temp + Integer.parseInt (s3);
8: S3=toBinaryString (temp);
9: end for
10: end Strategy

Step IV: Decoding of record
1: Strategy Decoding (b)
2: Encode. nit (cipher.DecryptMode, Mystery key);
3:Encrypt. nit (cipher.DecryptMode, Ensured key);
4: cis=new fileOutputStream (fis, encode);
5: fos=new fileOutputStream (dec);
6: byte [ ] b=new byte [8];
7: inti=cis.read (b);
8: while I! =-1 do
9: fos.write (b, 0, I);
10: i=cis.read (b);
11: end while
12: end Method

7. Experiment And Results

To evaluate the performance of the system, the encryption time, key generation time and decryption time are calculated. The time taken by enhanced KP-ABE outsourcing scheme is calculated on Integrated Development Environment (IDE) JAVA while the database is kept in MYSQL.

Encryption& Decryption

Step 1:User ID is allocated to each data owner and data receiver

Step 2: With OTP verification code data owner allow to upload a file and allocating separate folder for each data owners. Only authenticated user can upload the files.

Step 3 : Assign the attribute for each file, to generate single key using triple key. using that key the file willbe encrypted

Step 4 : Upload a encrypted file to be segmentated as six parts. Divided file to be stored in cloud storage(Using Amazon Ec2)

Step 5 : Authenticate user to decrypt the file with secret key Performance analysis is done using different file sizes and the results are obtained by noting down the time taken for encrypting those files with different sizes, time taken for decrypting those files and time taken for key generation. The original message and encrypted file is represented in fig 2&3.

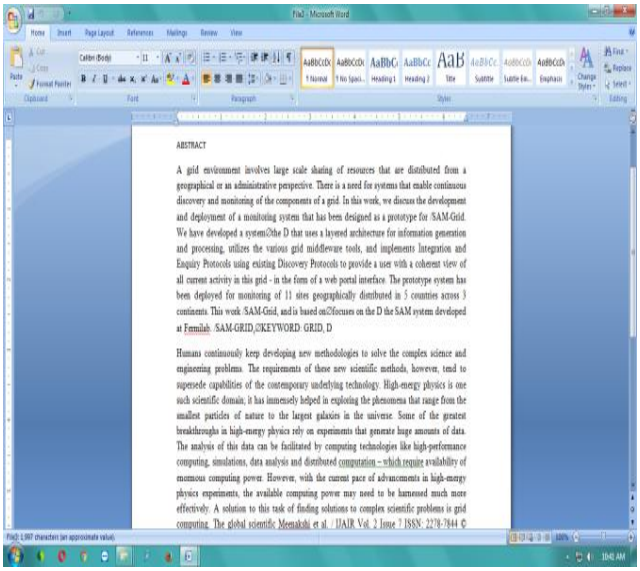


Fig.2: Shows plaintext

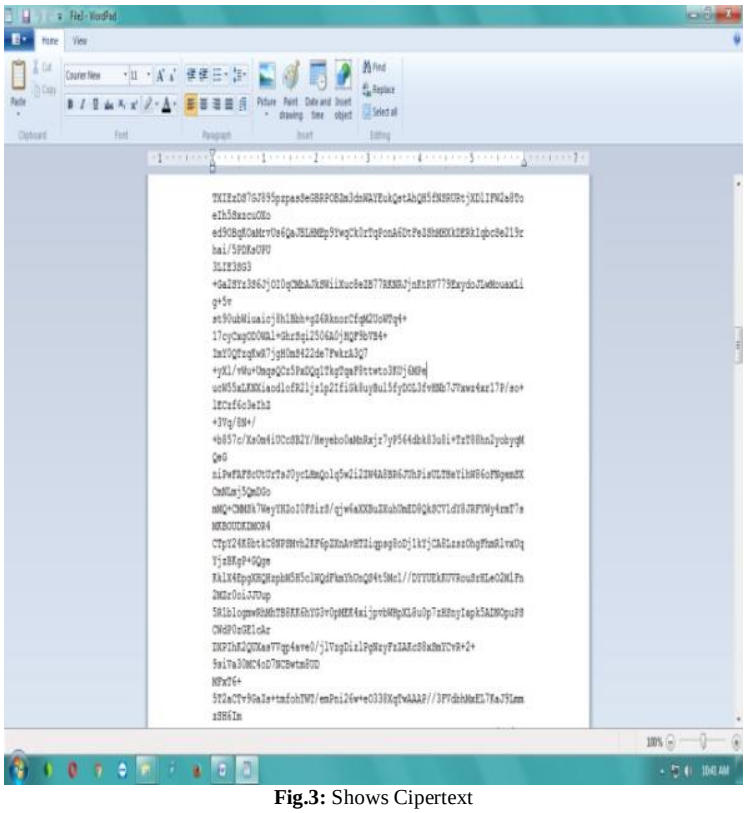


Fig.3: Shows Cipertext

To evaluate the performance of proposed algorithm, time taken to encrypt the file by using different file sizes—1 KB, 2 KB, 5 KB, 50 KB, 100 KB is considered. It was shown in below fig 4

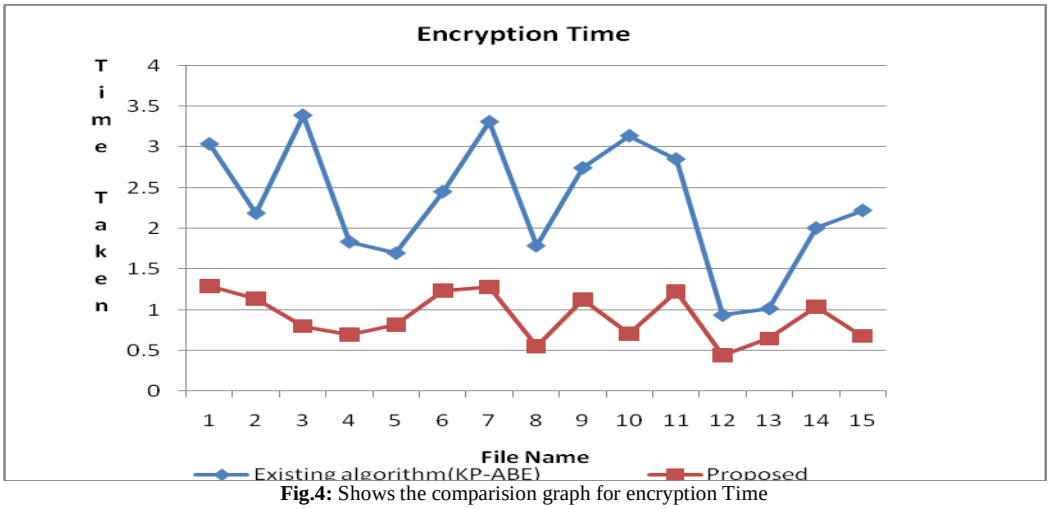


Fig.4: Shows the comparision graph for encryption Time

Key generation time is represented as to generate key for downloading file from the system. Here the file sizes used are 1KB, 2KB, 5KB, 50KB, and 100KB. And by using the same key authenticate user to decrypt the file with some specified time .key generation time and decryption process time it was shown in fig 5 and 6.

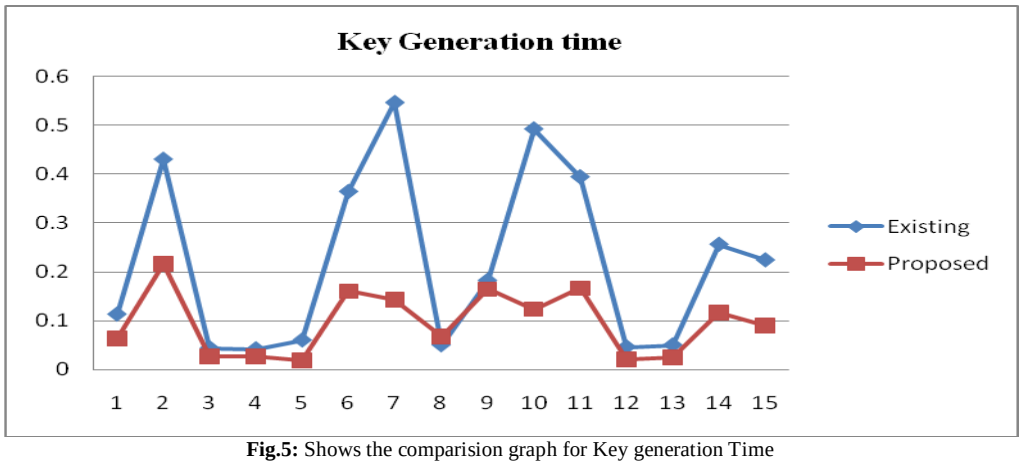


Fig.5: Shows the comparision graph for Key generation Time

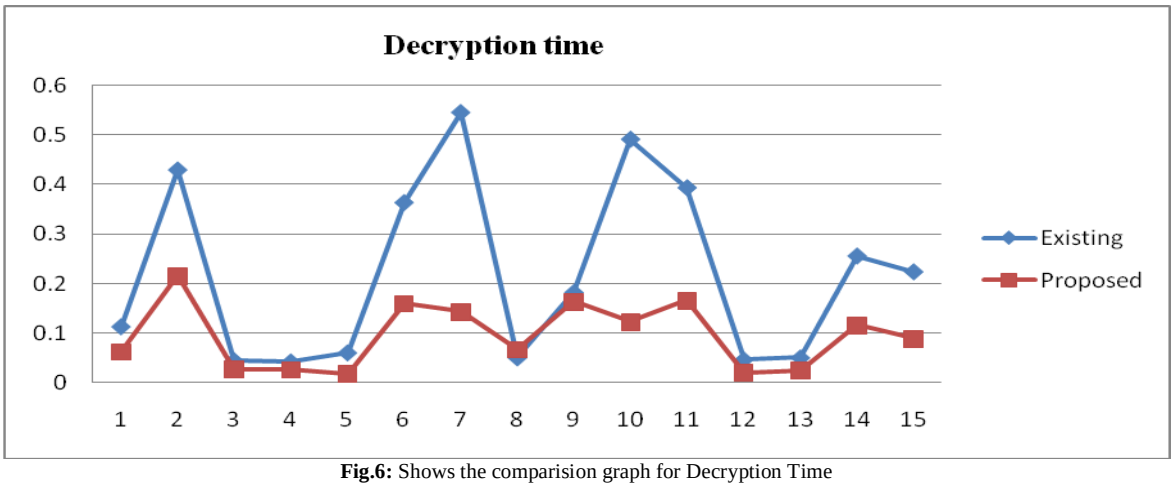


Fig.6: Shows the comparision graph for Decryption Time

8. Performance analysis

Here we are comparing the exising KP-ABE and proposed modified keypolicy attribute based encryption with different parameters such as keylength ,Data center,Block size ,secure access control .From the result we are achieved data confidentiality,efficiency ,flexbility,Level of security and encryption speed .our proposed work is more efficient than existing algorithm and is suitable for real time systems.

Parameters	Existing Algorithm KPABE	Proposed Algorithm Enhanced KPABE
Block-ciper	Binary	Binary
Key Length	128 bits, 192 bits and 256	1 – 4096 set of integers
Data Center	No	Yes
Data Tenant	Yes	Yes
Block size	128 bits	1024 bits
Efficiency	Average	Good
Flexibility	YES, Extended from 56 to 168 bits	YES, 256 key size is multiple of 64
Effectiveness	Slow	Efficient
Level of Security	Adequate Security	Highly Secure
Encryption Speed	Slow	High
Secured Access control	Low	High
Data Confidentiality	No	Yes
User Accountability	No	Yes

Fig.7: Performance analysis

9. Conclusion

Cloud computing has a potental for cost savings to the enterprises but the security risk are also enormous. Enterprise looking into cloud computing technology as a way to cut down on cost and increase profitability should seriously analyze the security risk of cloud computing. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. This proposed work provide security of user data from unauthorized user access in cloud storage and reduce the encryption time, key generation and decryption time.

References

[1] Lan Zhou, Vijay Varadharajan"Trust EnhancedCryptographic Role-Based Access Control for SecureCloud Data Storage" IEEE TRANSACTIONS ONINFORMATION FORENSICS AND SECURITY,VOL. 10, NO. 11, NOVEMBER 2015

[2] .J. F. Yang and Z. B. Chen, "Cloud computing Exploration and Security Issues," 2010 IEEE Worldwide Gathering on Computational Knowledge and Programming Building (CiSE), Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.

[3] Takabi, H., Joshi, J.B.D.: Security and protection challenges in cloud computing condition. IEEE Diary on Security and Protection 8(6) (November 2010)

[4] Yang, J., Chen, Z.: Cloud computing exploration and security issues. In: The Procedure of IEEE Universal Gathering on Computational Knowledge and Programming Building, pp. 1– 3 (2010)

[5] Kaitai Liang, Joseph K. Liu, Duncan S. Wong, Willy Susilo, "An Effective Cloud-based Revocable Character based Intermediary Re-encryption Plan for Open Mists Information Sharing", vol. 8712. Sep. 2014, pp. 257– 272.

[6] SADIKIN RIFKI, YOUNGHO Stop, SANGJAE MOON , " A Completely Secure Figure content Strategy Trait Based Encryption With A Tree-Based Access Structure".

[7] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), vol. 9327. Sep. 2015, pp. 146–166.

[8] Li M, Yu S, Cao N, Lou W. Authorized private keyword search over encrypted data in cloud computing. In 31st international conference on distributed computing systems (ICDCS) 2011 (pp. 383-92). IEEE.

[9] Y. Yang, J. K. Liu, K. Liang, K.- K. R. Choo, and J. Zhou, "Broadened intermediary helped approach: Accomplishing revocable fine-grained encryption of cloud information," in Proc. twentieth Eur. Symp. Res. Comput. Secur. (ESORICS), vol. 9327. Sep. 2015, pp. 146– 166.

[10] T. Jiang, X. Chen, J. Li, D. S. Wong, J. Mama, and J. Liu, "Clock: Secure and dependable cloud storage against information re-outsourcing," in Proc. tenth Int. Conf. Inf. Secur. Pract. Exper., vol. 8434. May 2014, pp. 346– 358.

[11] Li M, Yu S, Cao N, Lou W. Approved private catchphrase seek over scrambled information in cloud computing. In 31st worldwide meeting on circulated processing frameworks (ICDCS) 2011 (pp. 383-92). IEEE.

[12] Yang Y. Towards multi-client private watchword scan for cloud computing. In IEEE global meeting on cloud computing (CLOUD) 2011 (pp. 758-9). IEEE.

[13] Wang Q, Wang C, Ren K, Lou W, Li J. Empowering open auditability and information elements for capacity security in cloud computing. IEEE Exchanges on Parallel and Conveyed Frameworks. 2011; 22(5):847-59.

[14] Joseph K. Liu and Man Ho Au and Xinyi Huang," Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services" IEEE transactions on information forensics and security, vol. 11, no. 3, march 2016.

[15] M.Saraswathi, Dr.T.Bhuvaneswari" A Trusted Solution for Secure Outsourced Data Using Modified Key Policy AttributeBasedEncryption International Journal of Pure and Applied Mathematics Volume 118 No. 5 2018, 445-453