ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 7, Issue 2, February 2019**

# Assured Way to Manage Various Controls in Cloud

Dr.E.Sujatha[1], S.Divya[2], K.Atchaya [3], M.Sahana [4]

Associate Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India[1]

U.G Students, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India[2,3,4]

**ABSTRACT:** Cloud storage facilitates both individuals and enterprises to affordably share their knowledge over the Internet. However, this conjointly brings troublesome challenges to the access management of shared data since few cloud servers is totally sure. Cipher text-policy attribute-based encryption (CP-ABE) is a promising approach that enables the information homeowners themselves to position fine-grained and cryptographically-enforced access control over outsourced data. There is a tendency to gift secure and cost-efficient attribute based knowledge access control for cloud storage systems. A multi-authority CP-ABE scheme is constructed that features: 1) the system does not want a completely sure central authority, and all attribute authorities independently issue secret keys for users; 2) every attribute authority will dynamically take away any user from its domain such that those revoked users cannot access subsequently outsourced data; 3) cloud servers will update the encrypted knowledge from this time period to consequent one so that revoked users cannot access those antecedent offered data; and 4) the update of secret keys and cipher text is performed in an exceedingly public manner .The proposed scheme is proven secure in the random oracle model.

**KEYWORDS :** Access control, cloud storage, multi-authority,Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

## I. INTRODUCTION

Cloud storage is one of the major services provided by cloud computing. It enables data owners to remotely host their data by outsourcing them to cloud servers, which brings great convenience for both individuals and enterprises to share data over the Internet. However, this new paradigm challenges the approaches of traditional data access control scenarios, where a fully trusted server is in charge of implementing access control mechanisms, since the outsourced data might be sensitive and valuable for data owners, and few cloud servers can be fully trusted. Thus, to protect the security of outsourced data, data owners would like to place access policies over their data before outsourcing them to cloud servers. Among various solutions suggested for securing data sharing in cloud storage systems, attribute-based access control, which employs cipher text-policy attribute-based encryption (CP-ABE), is rather promising. In this setting, each user is described by a set of personal attributes and holds a secret key issued by an authority according to his/her attributes. A data owner defines an access policy over attributes and encrypts the data to be outsourced under this policy. Consequently, after outsourcing the encrypted data to cloud servers, only those users whose attributes satisfy the access policy can decrypt the outsourced data. This effectively prevents unauthorized users (including cloud servers) from accessing the outsourced data.

## II. LITERATURE SURVEY

Jiang hong Wei[1] proposed a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

cryptographically enhanced access control on the shared data. Identity-based encryption is a promising crypto-graphical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. Further more, concrete construction of RS-IBE is presented, and proved its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

Sebastian Lins[2] has proposed Cloud service certifications (CSC) for establishing trust, and increasing transparency of the cloud market. Several CSC have evolved, such as CSA STAR or Euro Cloud Star Audit. These CSC attempt to assure a high level of security, reliability, and legal compliance, for a validity period of one to three years. However, cloud services are part of an ever-changing environment, resulting from fast technology life cycles and inherent cloud computing (CC) characteristics, like on-demand provisioning and entangled supply chains. Hence, such long validity periods may put in doubt reliability of issued certifications. CSC criteria may no longer be met throughout these periods, for instance, due to configuration changes or major security incidents. Thus, continuous auditing (CA) of certification criteria is required to assure transparent, continuously reliable, and secure cloud services and to establish a trustworthy CSC after the initial certification process is accomplished.

Samee U. Khanwe[3] propose Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, files are divided into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Moreover, the nodes storing the fragments, are separated with certain distance by means of graph T-coloring to prohibit an attacker of guessing the locations of the fragments. Furthermore, the DROPS methodology does not rely on the traditional cryptographic techniques for the data security; thereby relieving the system of computationally expensive methodologies. It shows the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low. Also it compares the performance of the DROPS methodology with ten other schemes. The higher level of security with slight performance overhead was observed.

## III. PROPOSED SYSTEM

A multi authority CP-ABE scheme is used, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. This attribute revocation method is efficient because it has less communication cost and computation cost, and it can achieve both backward security (The revoked user cannot decrypt any new cipher text) and forward security (The newly joined user can also decrypt the previously published ciphertexts). In this scheme the server need not be trusted fully, because the server will not enforce the key update by each attribute authority.This scheme makes use of backward security even if the server is not semi-trusted. The proposed CP-ABE scheme is applied as the underlying technique to construct the secure data access control for multi-authority cloud storage systems.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

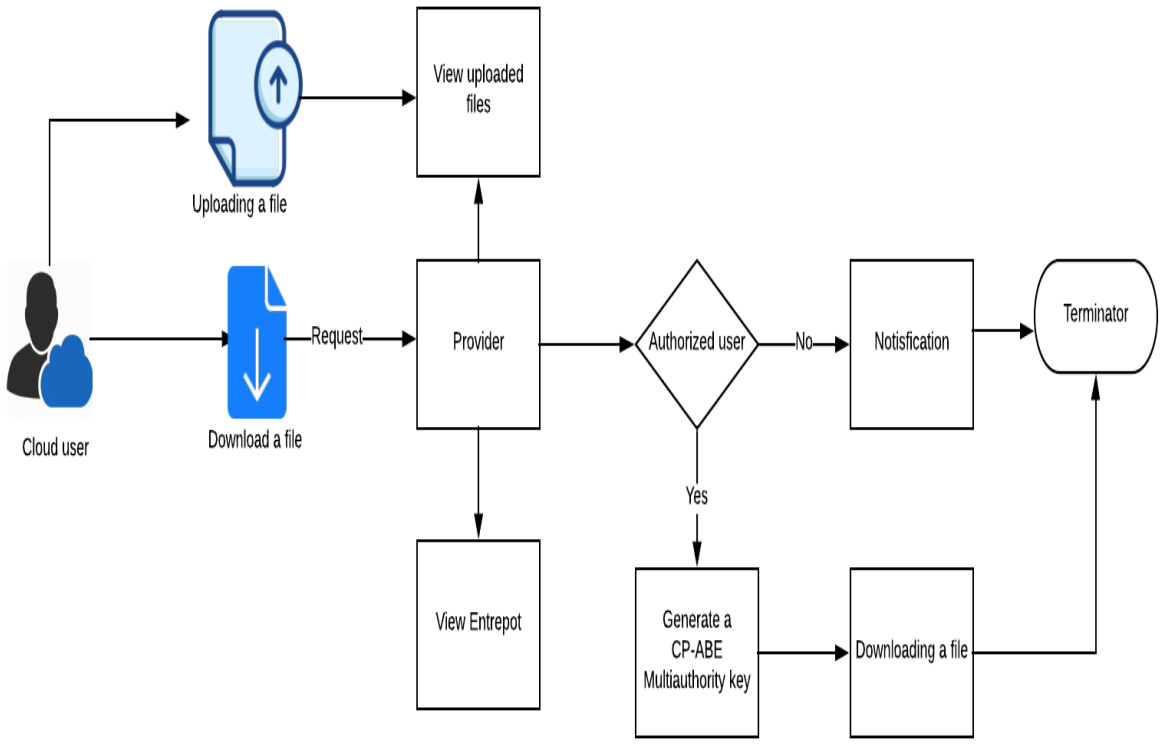
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

## IV. PROPOSED SYSTEM ARCHITECTURE DIAGRAM




## OUR MULTI-AUTHORITY CP-ABE SCHEME

The core building of our data access control scheme is given for cloud storage systems, a multiauthority CPABE scheme supporting efficient user revocation, and public ciphertext update.

**Our technique:**

A desirable multiauthority CP-ABE scheme should have the following features.

1) The public parameter should remain unchanged, and any string can be an attribute.

2) The revoked users can no longer decrypt those previously accessible data and subsequently encrypted data, namely, it should provide forward security and backward security simultaneously.

3) The ciphertext update should not involve secret information.

To this end, scheme upon large attribute universe CP-ABE schemes and utilize a binary tree to manage users' identifiers. Meanwhile, the lifetime of the system is divided into numerous discrete time periods, and each ciphertext is associated with a time period.We employ another binary tree in a different way to handle these time periods such that the ciphertext can be publicly updated from the current time period to the next one.Specifically speaking, each attribute authority $\delta$ maintains a binary tree $BT\,\delta$ with $N$ leaf nodes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

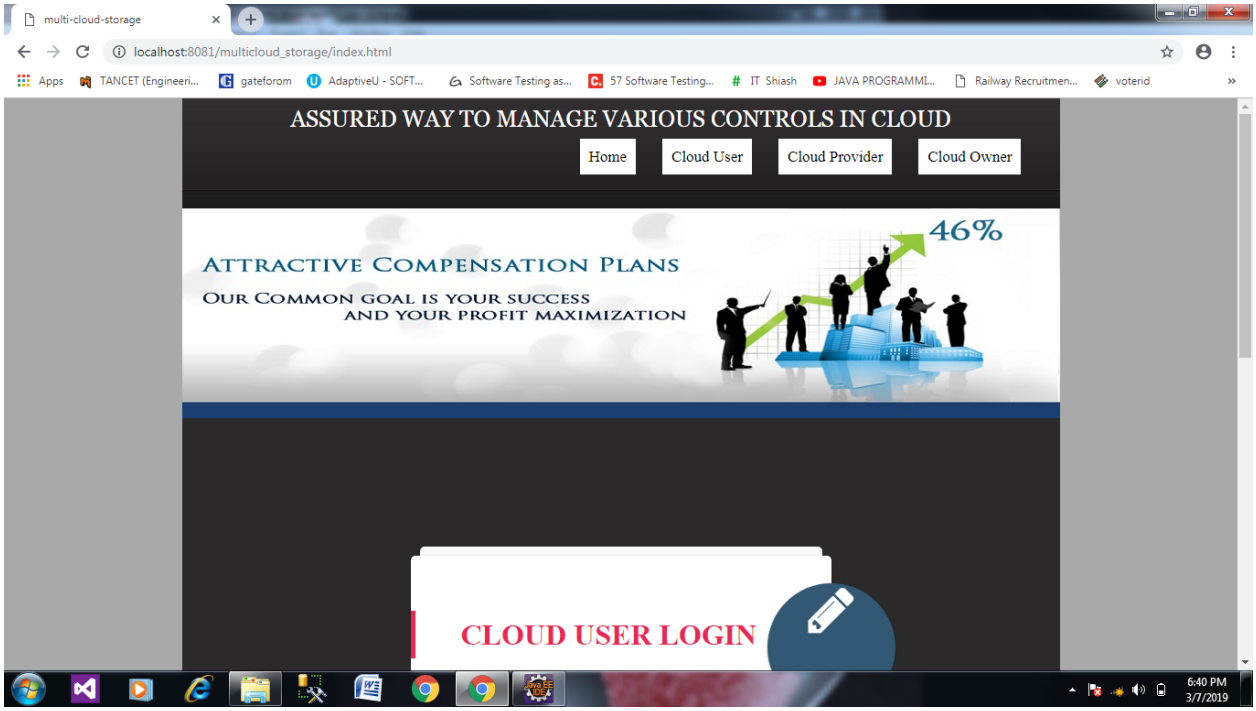
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

## V. OUTPUT SCREENS





| Cloud Provider | Storage Space | Storage Cost | Action | Request Action |
|---|---|---|---|---|
| null | 500GB | 8000 | Uplaod File | Send Request |
| null | 1000GB | 100000 | Uplaod File | Send Request |
| Atchaya | 800GB | 8000 | Uplaod File | Send Request |
| Atchaya2 | 1TB | 50000 | Uplaod File | Send Request |
| Atchaya | 2TB | 11000 | Uplaod File | Send Request |

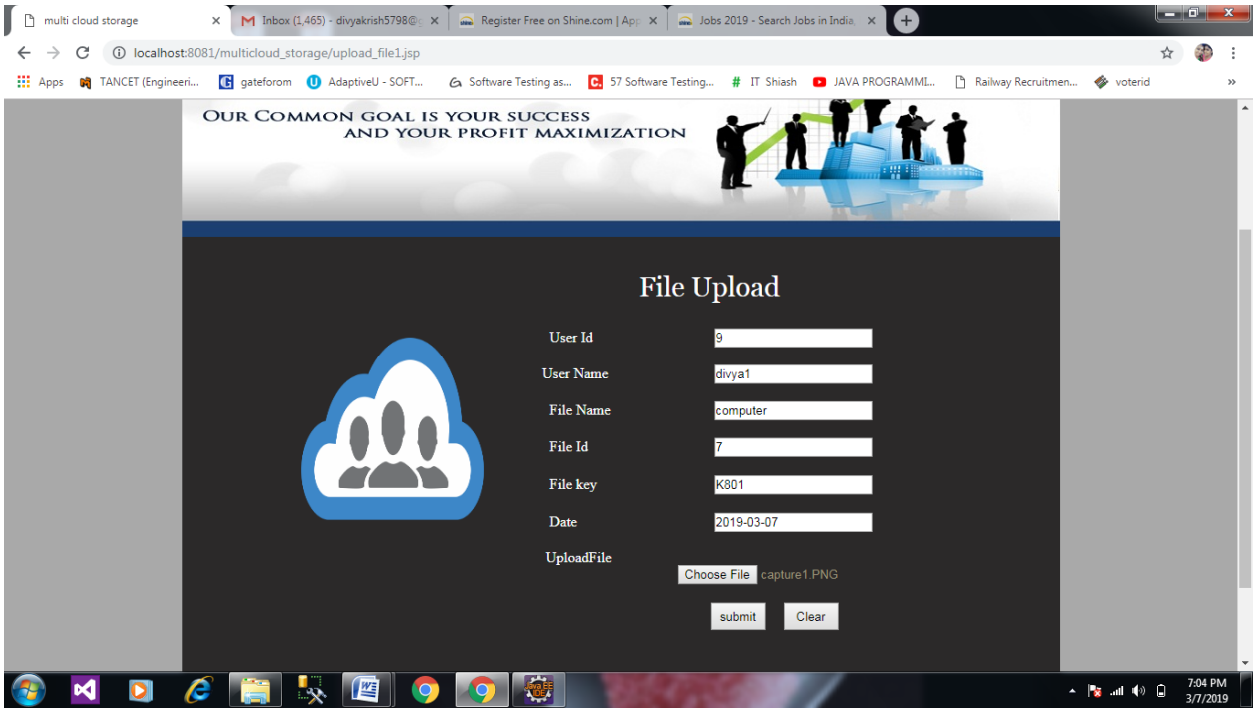
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

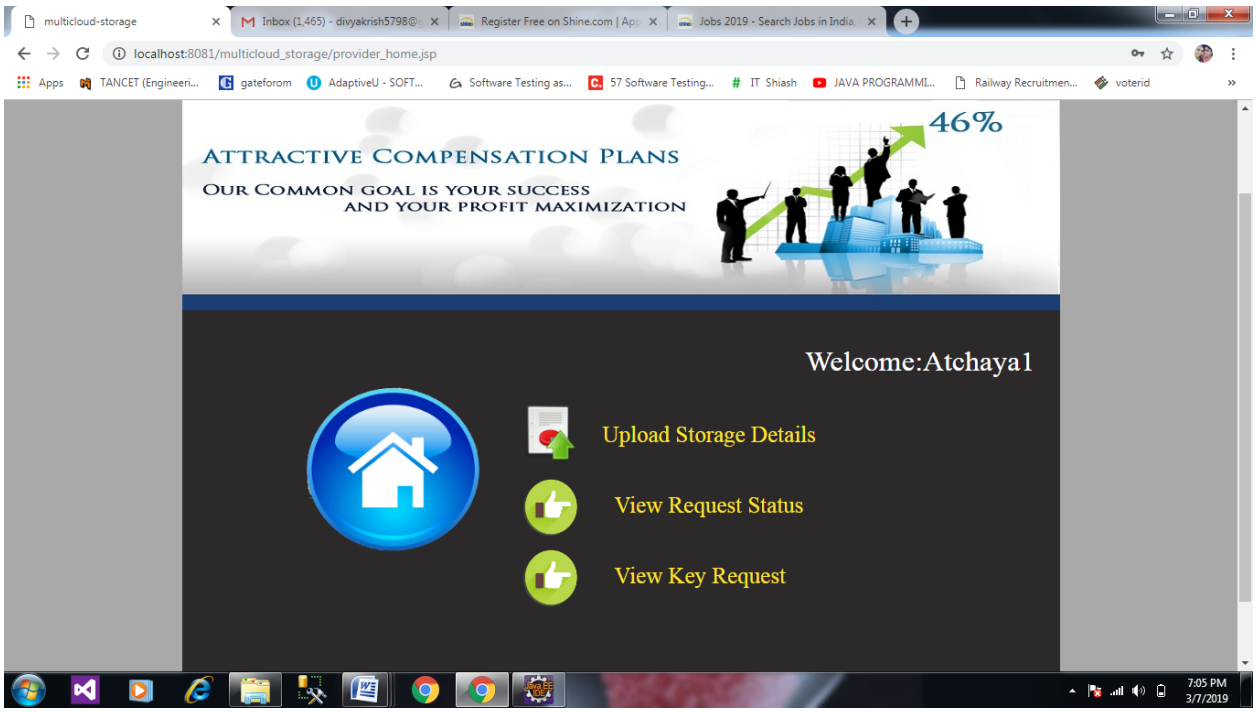
# International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 7, Issue 2, February 2019**



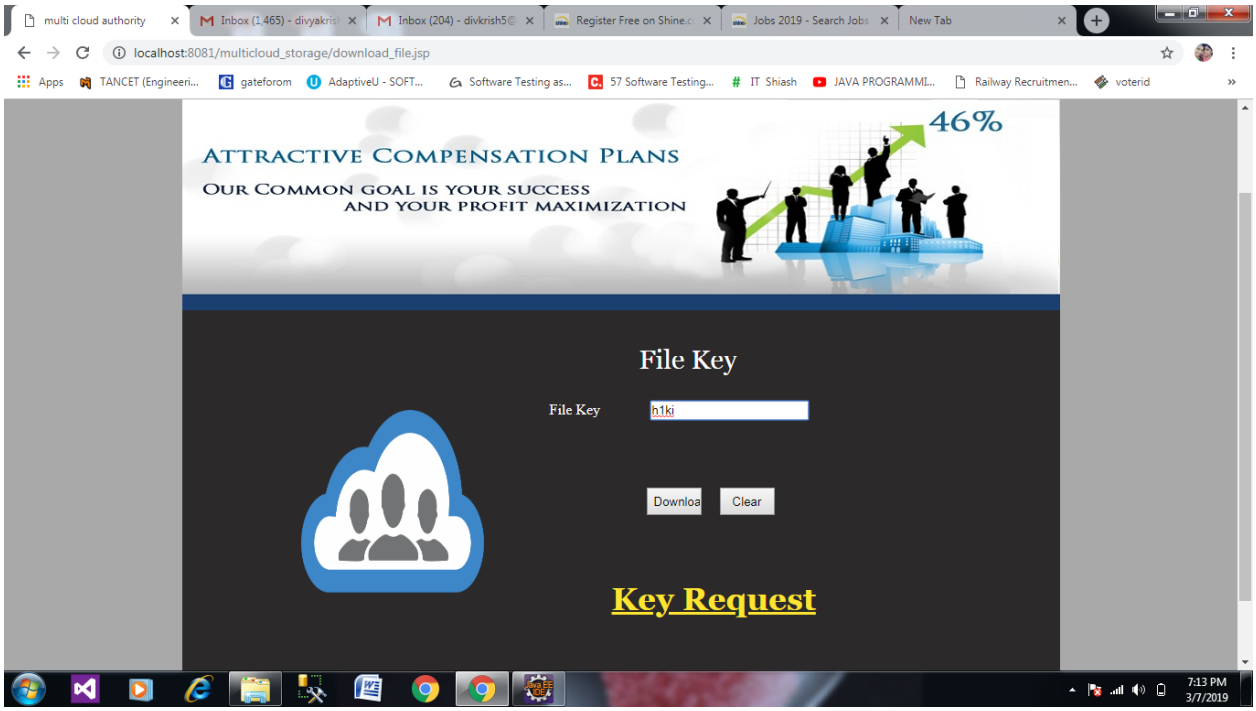
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019




## VI. CONCLUSION AND FUTURE WORK

The power of cloud computing is the ability to manage risks in some particular security issues. The algorithm suggested for data security shows its need. Security algorithm mentioned for encrytion and decryption can be implemented in future to enhance security framework over the network. In the future, At the cost of additional computation and communication overhead, the proposed scheme provides desirable security properties for practical applications. However, compared with those constructions providing the same security properties but built upon bilinear groups of Composite order, our scheme is more efficient.

## REFERENCES

[1] Secure and Efficient Attribute-Based Access Control for Multi authority Cloud Storage-(Jianghong Wei, Wenfen Liu, and Xuexian Hu ,IEEE SYSTEMS JOURNAL ,VOL.12, NO.2, JUNE 2018)
[2] Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing-(Sebastian Lins, Stephan Schneider, and Ali Sunyaev, IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 6, NO. 3, JULY-SEPTEMBER 2018)
[3] DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security-(Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, and Albert Y. Zomaya, Fellow, IEEE, Citation information: DOI 10.1109/TCC.2015.2400460, IEEE Transactions on Cloud Computing) .
[4] D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya,"Energy-efficient data replication in cloud computing datacenters," In IEEE Globecom Workshops, 2013, pp. 446 451.
[5] B. Grobauer, T.Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," IEEE Security and Privacy, Vol.9, No. 2, 2011, pp. 50-57.
[6] Y. Yang, X. Peng, and D. Fu, ''A framework of cloud service selection based on trust mechanism,'' Int. J. Ad Hoc Ubiquitous Comput., vol. 25, no. 3, pp. 109–119, 2017.
[7] L. Huang, S. Deng, Y. Li, J. Wu, J. Yin, and G. Li, ''A trust evaluation mechanism for collaboration of data-intensive services in cloud,'' Appl. Math. Inf. Sci., vol. 7, no. 1L, pp. 121–129, 2013.
[8] Y.-M. Tseng, T.-T. Tsai, S.-S. Huang, and C.-P. Huang, ''Identity-based encryption with cloud revocation authority and its applications,'' IEEE Trans. Cloud Comput., to be published, doi: 10.1109/TCC.2016.2541138.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Website: www.ijircce.com*

**Vol. 7, Issue 2, February 2019**

[9] J. H. Seo and K. Emura, ''Revocable identity-based encryption revisited: Security model and construction,'' in Proc. PKC, in Lecture Notes in Computer Science, vol. 7778, 2013, pp. 216–234.
[10] Q. Zheng, S. Xu, and G. Ateniese, ''VABKS: verifiable attributebased keyword search over outsourced encrypted data,'' in Proc. IEEE INFOCOM, Apr./May 2014, pp. 522–530.
[11] C. Guo et al., ''Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage,'' Future Gener. Comput. Syst., vol. 84, no. 7, pp. 190–199, 2018
[12] ] L. Guo, B. Lu, X. Li, and H. Xu, ''A verifiable proxy re-encryption with keyword search without random oracle,'' in Proc. Int. Conf. Comput. Intell. Secur., 2013
[13] J. Li, X. Lin, Y. Zhang, and J. Han, ''KSF-OABE: Outsourced attributebased encryption with keyword search function for cloud storage,'' IEEE Trans. Services Comput., vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017
[14] ] M. Li, S. Yu, N. Cao, and W. Lou, ''Authorized private keyword search over encrypted data in cloud computing,'' in Proc. IEEE 31st Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2011
[15] S. Wang, J.Zhou, Liu JK, et al. An Efficient File Hierarchy AttributeBased Encryption Scheme in Cloud Computing[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(6):1265-1277.
[16] Wang G, Liu Q, Wu J, et a1.Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers[J] . Computers & Security忡2011,30 (5):320 -331.
[17] J. Baek, R. Safavi-Naini, and W. Susilo, ''Public key encryption with keyword search revisited,'' in Proc. Int. Conf. ICCSA, vol. 5072. Perugia, Italy, Jun./Jul. 2008, pp. 1249–1259.
[18] P. Xu, Q. Wu, W. Wang, W. Susilo, J. Domingo-Ferrer, and H. Jin, ''Generating searchable public-key ciphertexts with hidden structures for fast keyword search,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 1993–2006, Sep. 2015.
[19] L. Ibraimi, S. Nikova, P. Hartel, and W. Jonker, ''Public-key encryption with delegated search,'' in Applied Cryptography and Network Security (Lecture Notes in Computer Science), vol. 6715. Heidelberg, Germany: Springer, 2011, pp. 532–549.
[20] Y. H. Hwang and P. J. Lee, ''Public key encryption with conjunctive keyword search and its extension to a multi-user system,'' in Pairing-Based Cryptography—Pairing (Lecture Notes in Computer Science), vol. 4575. Berlin, Germany: Springer, 2007, pp. 2–22.