International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Secure Data Group Sharing with Attribute and Time based encrypted data access over cloud

Ms. B.N.V.D.Bhavani[1], Dr. A. Veerabhadra Rao[2]

#1Student, Department Of Computer Science Engineering,Jogaiah Institute of Technology and Sciene College of Engineering, Kalagampudi, Near Palakol, West Godavari District, Andhra Pradesh – 534268 .

#2HOD, Department Of Computer Science Engineering,Jogaiah Institute of Technology and Sciene College of Engineering, Kalagampudi, Near Palakol, West Godavari District, Andhra Pradesh – 534268 Email:- badrialumuri2005@gmail.com

Abstract_ Cloud computing has gotten progressively prevalent among clients and organizations around the globe. Albeit cryptographic systems can give information assurance to clients out in the open cloud, a few issues additionally stay tricky, for example, secure information bunch scattering and fine-grained get to control of time-delicate information. In this paper, we propose a character based information bunch sharing and spread plan in broad daylight cloud, in which information proprietor could communicate encoded information to a gathering of beneficiaries one after another by indicating these collectors' personalities in an advantageous and secure manner. So as to accomplish secure and adaptable information bunch dispersal, we embrace quality based and coordinated discharge contingent intermediary re-encryption to ensure that lone information disseminators whose properties fulfill the entrance arrangement of scrambled information can spread it to different gatherings after the discharging time by assigning a re-encryption key to cloud server. The re-encryption conditions are related with qualities and discharging time, which enables information proprietor to implement fine-grained and planned discharge get to authority over scattered ciphertexts.

Index Terms—Attribute-based encryption, conditional proxy re-encryption, timed-release encryption, cloud computing

1.INTRODUCTION

Cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

The cloud computing benefits individual users and enterprises with convenient access, increased operational eciencies and rich storage resources by combining a set of existing and new techniques from research areas such as service-oriented architectures and virtualization. Although the great benefits brought by cloud computing are exciting for users, security problems may somehow impede its quick development .Currently, more and more users would outsource their data to cloud service provider (CSP) for sharing. However, the CSP which deprives data owners direct control over their data is assumed to be honest-but- curious, that may prompt security concerns. These security matters existing in public cloud motivate the requirement to appropriately keep data confidential. Several schemes exploiting cryptographic mechanisms to settle the security problems have been proposed. In order to guarantee secure data group sharing, identity-based broadcast encryption (IBBE) scheme [11] is employed in public cloud. The data owners could broadcast their encrypted data to a group of receivers at one time and the public key of the user can be regarded as email, unique id and user- name Hence, by using an identity, data owner can share data with other group users in a convenient and secure manner. Attribute- based encryption (ABE) is one of new cryptographic mechanisms used in cloud to reach flexible and fine-grained secure data group sharing. Especially, cipher text-policy ABE (CP-ABE) allows data owners to encrypt data with an access policy such that only users whose attributes satisfy the access policy can decrypt the data [12]. Time-sensitive data such as a business plan and a tender, is a special data in cloud which requires time-based exposing [2] It means that data owner may want different users to disseminate data after different time. For instance, data owner may share sensitive business plan with directors, and he hopes these directors only can disseminate business plan to managers at an early time and then to other employees at last.

2.LITERATURE SURVEY

1.TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud

Description : By integrating TRE and CP-ABE in public cloud storage, an effcient scheme to realize secure negrained access control for time-sensitive data. In the proposed scheme, the data owner can autonomously designate intended users and

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

their relevant access privilege releasing time points. Besides realizing the function, it is proved that the negligible burden is upon owners, users and the trusted CA. It is presented how to design access structure for any potential timed release access policy, especially embedding multiple releasing time points for different intended users. Timed-Release Encryption (TRE) becomes a promising primitive, in which, a trusted time agent, instead of data owners, uniformly executes the timedrelease function.

2. RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage

Description : To address the single-point performance bottleneck of key distribution existed in the existing schemes, here propose a robust and efficient heterogeneous framework with single CA (Central Authority) and multiple AAs (Attribute Authorities) for public cloud storage. The heavy load of user legitimacy verification is shared by multiple AAs, each of which man- ages the universal attribute set and is able to independently complete the user legitimacy verification, while CA is only responsible for computational tasks. This is the first work that proposes the heterogeneous access control framework to address the low efficiency and single-point performance bottleneck for cloud storage. It is reconstructed the CP-ABE scheme to fit our proposed framework and propose a robust and high- efficient access control scheme, meanwhile the scheme still preserves the fine granularity, flexibility and security features of CP-ABE.

3.EXISTING SYSTEM

- There have been numerous works on secure data group sharing and dissemination in public cloud based on various cryptographic primitives [14], such as PRE [15,16,17], broadcast encryption [18,19] and ABE [20,21]. Ulybyshev et al. [22] designed a solution that ensures privacy preserving data sharing based on the role-based access control and cryptographic capabilities of client's browser. Popa et al. [23] proposed CryptDB based on order preserving encryption and homomorphic encryption to guarantee data confidentiality of database in public cloud.

- Zhou et al. [24] proposed a secure data group sharing scheme based on IBBE algorithm, in which data owner can broadcast encrypted data to a group of users at

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

the same time. In order to achieve data collaboration and dissemination, this scheme adopted the PRE technique to allow an authorized proxy to convert an IBBE cipher text into an identity-based encryption (IBE) cipher text. Hence, the intended receiver can decrypt the IBE cipher text. However, this PRE scheme only allows the re-encryption procedure to be executed in an all-or-nothing manner, which means the proxy can either re-encrypt all the initial cipher texts or none of them. The CPRE scheme could allow users to generate a re-encryption key associated with a condition and only the encrypted data meeting the condition can be re-encrypted [25,26].

4.PROPOSED WORK

The essential objective of our plan is to accomplish fine-grained and coordinated discharge information bunch dispersal. Fig. 1 shows the framework model of our plan, which comprises of the accompanying framework elements.

 The focal power (CA) is a completely confided in au-thority running on confided in cloud stage with adaptability and versatility that oversees and dis-tributes open/mystery enters in the framework, including creates framework parameters to instate sys-tem and produces private keys and quality keys with clients' character and characteristics. Likewise, it goes about as a confided in time specialist to distribute time token at each pre-characterized time.

 The CSP is a semi-confided in substance that has rich stockpiling limit and calculation influence to master vide information sharing administrations in broad daylight cloud. It is accountable for controlling the gets to from outside us-ers to the put away information and giving compare ing administrations. At the point when it gets the solicitation of information re-encryption, it is answerable for creating a re-scrambled ciphertext with re-encryption key from information disseminator. Consequently, CSP stores initial ciphertexts, yet in addition re-scrambled ciphertexts.

 The information proprietor wishes to redistribute the information into cloud for comfort of gathering sharing and dissemination. The information proprietor is accountable for encrypting information for a lot of collectors. On the off chance that the information proprietor has the prerequisite to confine his information to be dispersed by some particular individuals after some particular time, the information

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

proprietor can characterize at-tribute-based and planned discharge get to approach, and uphold it all alone information by scrambling the information under the arrangement before re-appropriating it.

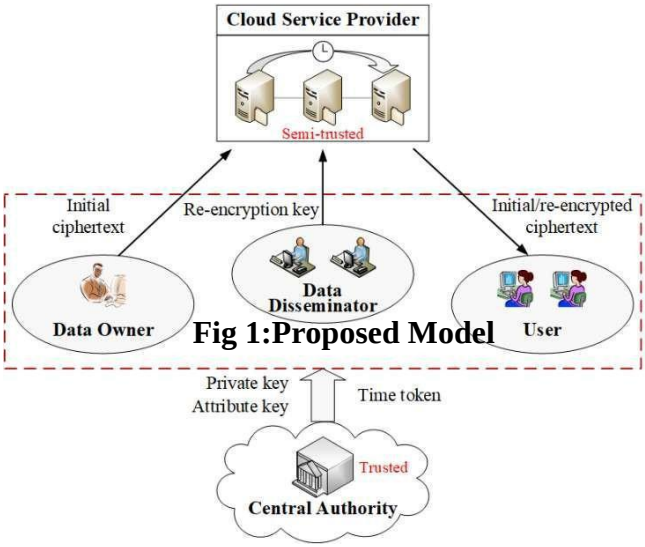


Fig 1:Proposed Model

 The data disseminator is the person who wishes to share data owner's data with other people (e.g. his friends, family members, colleagues). For security and access control considerations, data dissemina-tor must be one of intended receivers defined by the data owner, who could decrypt the initial ci-phertexts. The data disseminator can generate re-encryption keys, and then send data re-encryption requests with these keys to the CSP to disseminate data owner's data to others. Only the attributes of data disseminator satisfy access policy and the pre-determined time arrives, data re-encryption request can be successfully executed by CSP. The user is the ciphertexts receiver who can access the outsourced data. The user is able to decrypt the initial and re-encrypted ciphertexts if he is the in-tended receiver defined by the data owners or data disseminators.

International Journal of Research
Available at
https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

5.RESULTS AND DISCUSIONS

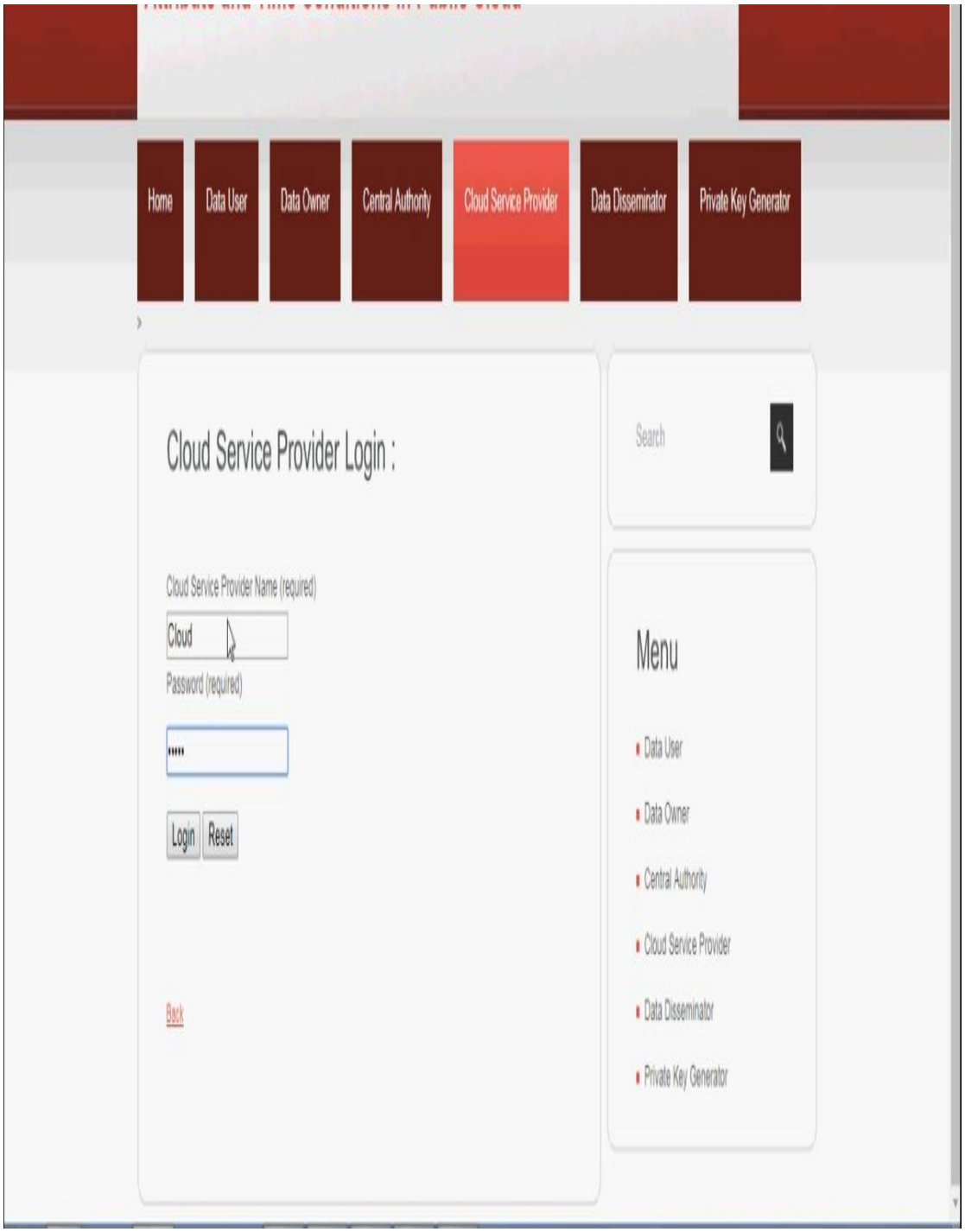


Fig 1:Cloud Server Provide Login Page

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

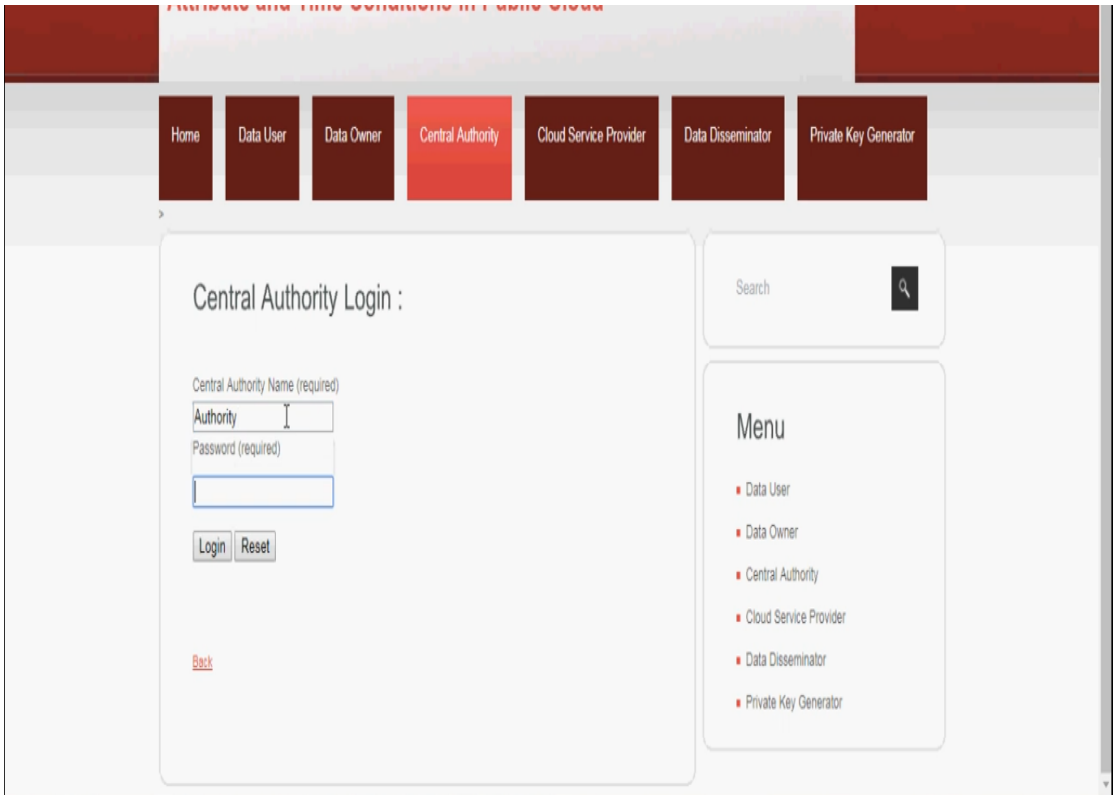
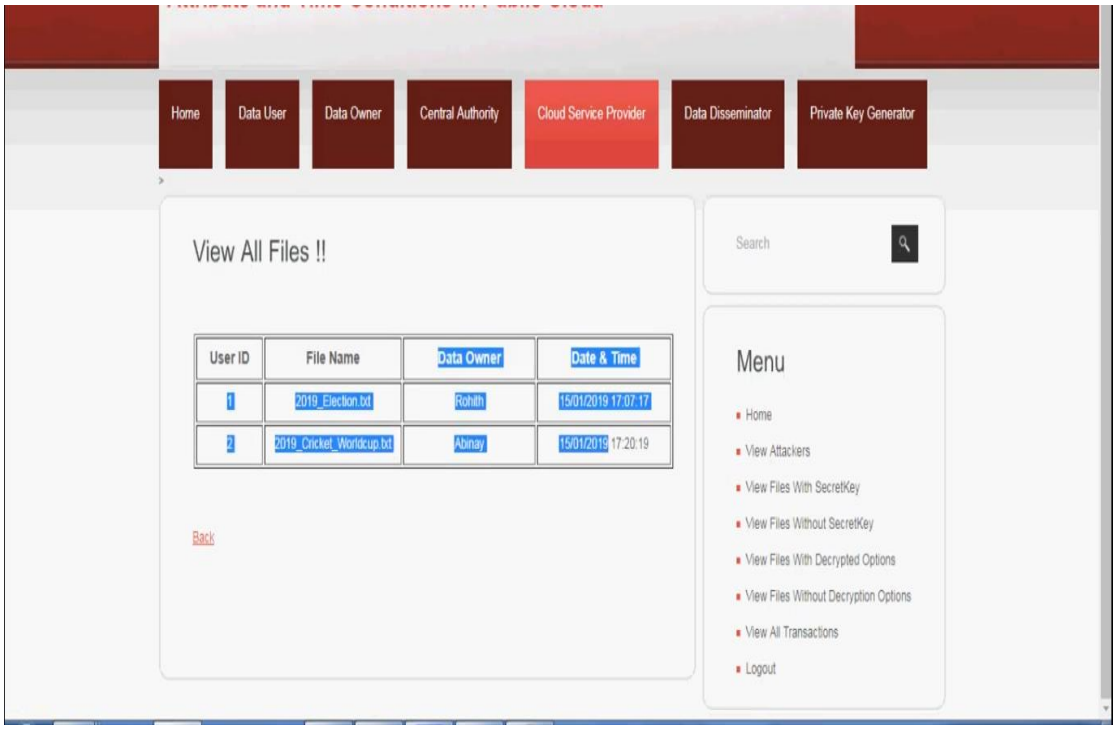


Fig 2: central authority page



e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Fig 3: view all files

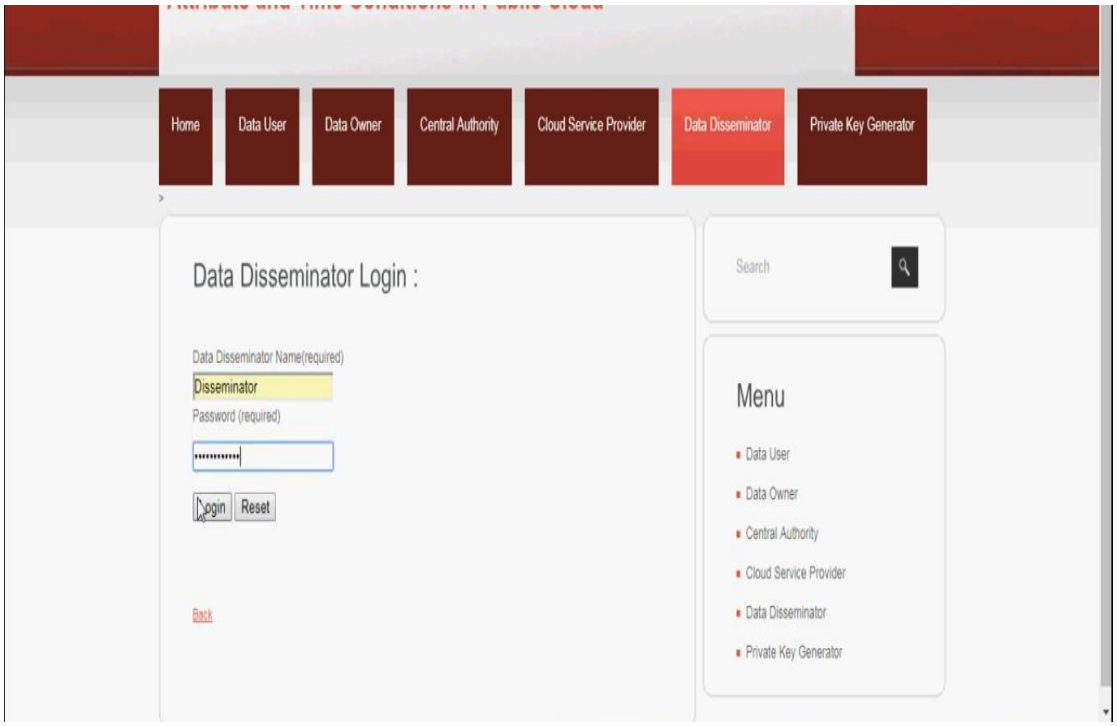


Fig 4: data disseminator page

6.CONCLUSION

In this paper, propose a secure information bunch sharing and scattering plan out in the open cloud dependent on at-tribute-based and planned discharge restrictive personality based communicate PRE. Our plan enables clients to impart information to a gathering of beneficiaries by utilizing character, for example, email and username at once, which would ensure information sharing security and accommodation out in the open cloud. In addition, with the use of fine-grained and planned discharge CPRE, our plan enables information proprietors to custom access arrangements and time trapdoors in the ciphertext which could restrain the dispersal conditions while re-appropriating their information. The CSP will re-encode the figure message effectively just when the qualities of information disseminator related with the re-encryption key fulfill get to strategy in the underlying ciphertext and the time trapdoors in the underlying figure content are uncovered. We lead our tests with matching based cryptography library. The hypothetical analaysis and trial results have demonstrated the security and effectiveness of our plan

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, ―Security Challenges for the Public Cloud,‖ *IEEE Internet Computing*, vol. 16, no. 1, pp. 69-73, 2012.

[2] C. Delerablée, ―Identity-based Broadcast Encryption with Constant Size Ciphertexts and Private Keys,‖ *Proc. the 13th International Confer- ence on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007)*, pp. 200-215, 2007.

[3] F. Beato, S. Meul, and B. Preneel, ―Practical Identity-based Private Sharing for Online Social Networks,‖ *Computer Communications*, vol. 73, pp. 243-250, 2016.

[4] J. Bethencourt, A. Sahai, and B. Waters, ―Ciphertext-policy Attribute- based Encryption,‖ *Proc. the 28th IEEE Symposium on Security and Pri- vacy (S&P 2007)*, pp. 321-334, 2007.

[5] Z. Wan, J. Liu, and R. Deng, ―HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Compu- ting,‖ *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 743-754, 2012.

[6] H. Hu, G. Ahn, and J. Jorgensen, ―Multiparty Access Control for Online Social Networks: Model and Mechanisms,‖ *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1614-1627, 2013.

[7] M. Blaze, G. Bleumer, and M. Strauss, ―Divertible Protocols and Atomic Proxy Cryptography,‖ *Proc. Advances in Cryptology- EUROCRYPT 1998 (EUROCRYPT '98)*, pp.127-144, 1998.

[8] D. Tran, H. Nguyen, W. Zha, and W. Ng, ―Towards Security in Shar- ing Data on Cloud-based Social Networks,‖ *Proc. the 8th International Conference on Information, Communications and Signal Processing (ICICS2011)*, pp. 1-5, 2011.

[9] J. Weng, R. Deng, X. Ding, C. Chu, and J. Lai, ―Conditional Proxy Re-Encryption Secure Against Chosen-ciphertext Attack,‖ *Proc. the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (CCS 2009)*, pp. 322-332, 2009.

[10] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, ―Conditional Identity- based Broadcast Proxy Re-encryption and its Application to Cloud Email,‖ *IEEE Transactions on Computers*, vol. 65, no. 1, pp. 66-79, 2016.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 11
October 2019

Author's Profile

Ms. B.N.V.D.Bhavani, B.Tech in computer science and engineering from SWARNANDHRA ENGINEERING COLLEGE, affiliated to JNTU, Kakinada in 2016 , pursuing M.Tech in Computer science and engineering from JOGAIAH INSTITUTE OF TECHNOLOGY AND SCIENCE COLLEGE OF ENGINEERING affiliated to the JNTU, Kakinada in 2017-19

Dr. A. Veerabhadra Rao M.Tech., (Ph.D.,),
Head of Department,Computer Science Engineering Department
Jogaiah Institute of Technology and Sciene College of Engineering, Kalagampudi, Near Palakol, West Godavari District, Andhra Pradesh– 534268