iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 Issue: IV Month of publication: April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4331

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887*
*Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com*

# Identity based Encryption Technique for Secure Data Sharing in Public Cloud

K. Praveen Kumar[1], K. Nagabrunda[2], B. Navya[3], M.Sowmya[4], G. Praneeth Yadav[5]
*[1]Assistant Professor, Vignan Institute of Technology & Science*
*[2, 3, 4,5]CSE, Vignan Institute of Technology & Science, Hyderabad*

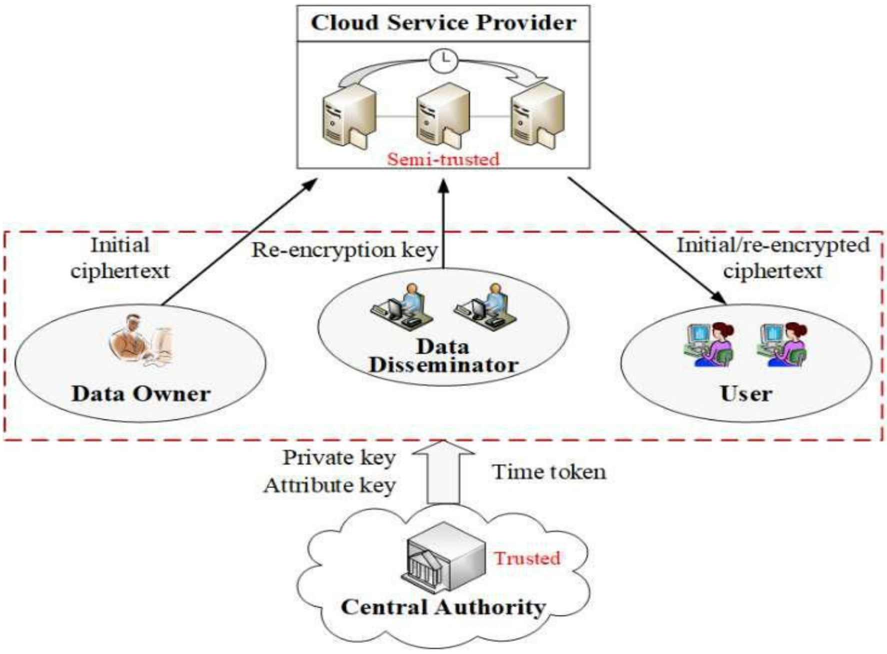
***Abstract: Cloud computing has become increasingly popular among users and businesses around the world. Although cryptographic techniques can provide data protection for users in public cloud, several issues also remain problematic, such as secure data group dissemination and fine-grained access control of time-sensitive data. Data users can search all files uploaded by data owners. He or she can send request to admin. Then admin will send the search key. After entering the search key, He or she can view the file.***

## I.INTRODUCTION

Cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. The cloud computing benefits individual users and enterprises with convenient access, increased operational efficiencies 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

## II. OBJECTIVE

Cloud computing has become increasingly popular among users and businesses around the world. Although cryptographic techniques can provide data protection for users in public cloud, several issues also remain problematic, such as secure data group dissemination and fine-grained access control of time-sensitive data. Data users can search all files uploaded by data owners. He or she can send request to admin. Then admin will send the search key. After entering the search key, He or she can view the file.



## III. PROPOSAL

In this paper, we propose a secure data group sharing and dissemination scheme with attribute and time conditions in public cloud. The main contributions of our scheme are as follows:

*A.* We employ IBBE technique to achieve secure data group sharing in public cloud, which allows data owner to outsource encrypted data to semi-trusted cloud and share it with a group of receivers at one time. It is more convenient that email and username could be used as public keys for users.

*B.* We design an access policy embedding releasing time and take the advantages of attribute-based CPRE, to achieve fine-grained and timed-release data group dissemination. The CSP can re-encrypt initial cipher texts for data disseminator after the designate time if his attributes associated with the re-encryption key satisfy the access policy in the cipher texts.

*C.* We analyze the security of our proposed scheme, and conduct a detailed theoretical and experimental analysis. The results show that our scheme makes a tradeoff between computational overhead and expressive dissemination conditions, and performs significantly better in data group sharing and dissemination in public cloud.

## IV. CONCLUSIONS

In this paper, we propose a secure data group sharing and dissemination scheme in public cloud based on attribute-based and timed-release conditional identity based broadcast PRE. Our scheme allows users to share data with a group of receivers by using identity such as email and username at one time, which would guarantee data sharing security and convenience in public cloud. Besides, with the usage of fine-grained and timed-release CPRE, our scheme allows data owners to custom access policies and time trapdoors in the cipher text which could limit the dissemination conditions when outsourcing their data. The CSP will re-encrypt the cipher text successfully only when the attributes of data disseminator associated with the re-encryption key satisfy access policy in the initial cipher text and the time trapdoors in the initial cipher text are exposed. We conduct our experiments with pairing-based cryptography library. The theoretical analysis and experiment results have shown the security and efficiency of our scheme.

## REFERENCES

[1] Varghese, Blesson, and Rajkumar Buyya. ―Next Generation Cloud Computing: New Trends and Research Directions.‖ Future Generation Computer Systems, vol. 79, 2018, pp. 849–861., doi:10.1016/j.future.2017.09.020.

[2] Wei, Jianghong, et al. ―Secure Data Sharing in Cloud Computing Using Revocable-Storage IdentityBased Encryption.‖ IEEE Transactions on Cloud Computing, 2016, pp. 1–1., doi:10.1109/tcc.2016.2545668

[3] Ma, Sha. ―Identity-Based Encryption with Outsourced Equality Test in Cloud Computing.‖ Information Sciences, vol. 328, 2016, pp. 389–402., doi:10.1016/j.ins.2015.08.053.

[4] Xin Dong, Jiadi Yu, Yanmin Zhu, Yingying Chen, Yuan Luo, Minglu Li, SECO: Secure and scalable data collaboration services in cloud computing, Computers & Security, Volume 50, 2015, Pages 91-105, ISSN 0167-4048

[5] Daniel, Renu Mary, et al. ―Analysis of Hierarchical Identity Based Encryption Schemes and Its Applicability to Computing Environments.‖ Journal of Information Security and Applications, vol. 36, 2017, pp. 20–31., doi:10.1016/j.jisa.2017.07.005.

[6] Boneh, Dan, and Matt Franklin. ―Identity-Based Encryption from the Weil Pairing.‖ Advances in Cryptology — CRYPTO 2001 Lecture Notes in Computer Science, 2001, pp. 213–229., doi:10.1007/3- 540-44647-8_13.

[7] Boldyreva, Alexandra, et al. ―Identity-Based Encryption with Efficient Revocation.‖ Proceedings of the 15th ACM Conference on Computer and Communications Security - CCS '08, 2008, doi:10.1145/1455770.1455823.

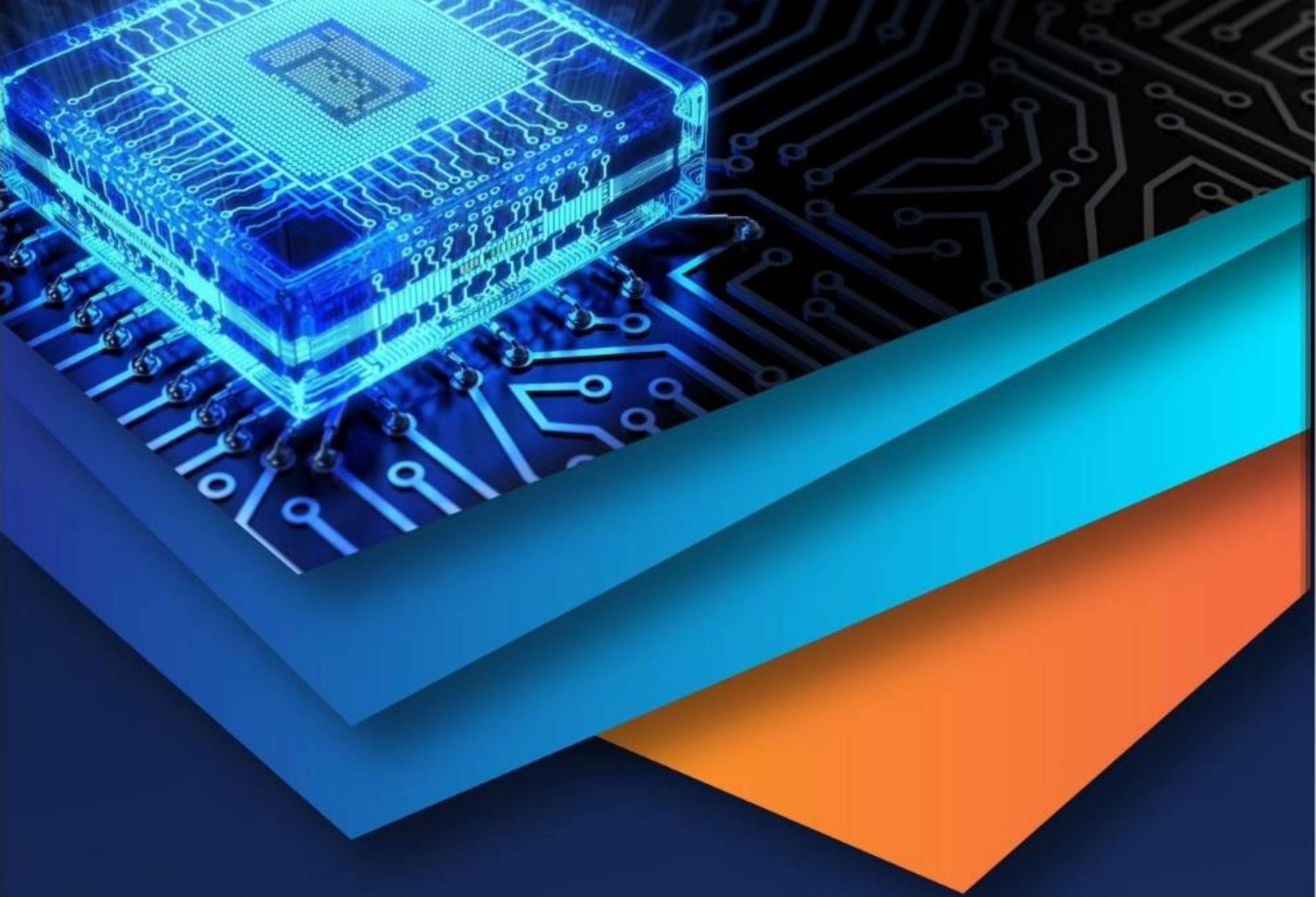
[8] Libert, Benoît, and Damien Vergnaud. ―AdaptiveID Secure Revocable Identity-Based Encryption.‖ Topics in Cryptology – CT-RSA 2009 Lecture Notes in Computer Science, 2009, pp. 1–15., doi:10.1007/978-3- 642-00862-7_1.

[9] Seo, Jae Hong, and Keita Emura. ―Revocable Identity-Based Encryption Revisited: Security Model and Construction.‖ Public-Key Cryptography – PKC 2013 Lecture Notes in Computer Science, 2013, pp. 216–234., doi:10.1007/978-3-642-36362-7_14.

[10] Liang, Kaitai, et al. ―An Efficient Cloud-Based Revocable Identity-Based Proxy Re-Encryption Scheme for Public Clouds Data Sharing.‖ Computer Security - ESORICS 2014 Lecture Notes in Computer Science, 2014, pp. 257–272., doi:10.1007/978-3-319-11203- 9_15.

[11] Qin, Baodong, et al. ―Related-Key Secure Key Encapsulation from Extended Computational Bilinear Diffie–Hellman.‖ Information Sciences, vol. 406-407, 2017, pp. 1–11., doi:10.1016/j.ins.2017.04.018.

[12] Wang C, Li Y, Xia X, Zheng K. An Efficient and Provable Secure Revocable Identity-Based Encryption Scheme. Xia C-Y, ed. PLoS ONE. 2014;9(9):e106925. doi:10.1371/journal.pone.0106925.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY