iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** X **Month of publication:** October 2018

DOI:

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 X, Oct 2018- Available at www.ijraset.com

Captcha based an Efficient and Fine- Grained Big Data Access Control Scheme with Hidden Policy

DR. Chandra Blessie [1], Nandhana.R [2]
[1]*Associate Professor,* [2]*Research Scholar, Department of Computer Application, Nehru College of Management, Coimbatore*

Abstract: Computer security also known as cyber security. Huge amount of big data becomes a very challenging issue it is stored in cloud with (CP-ABE). This paper propose that fine gained two-factor big data. Data access control protocol for web-based cloud computing by using captcha this paper also dials about an efficient and fine-grained data access control for big data.

I. INTRODUCTION

First time CAPTCHA was invented in 2000 at Carnegie Mellon University by John Langford CAPTCHAS are a kind of Turing test quite simply , end users are asked to perform some task that a software both cannot do - test often involve JPEG or Image, because while dots can identify the existence of an image by reading source code, they cannot tell what that image depicts because some CAPTCHA image are difficult to interpret, users are usually given the option to request a new test.

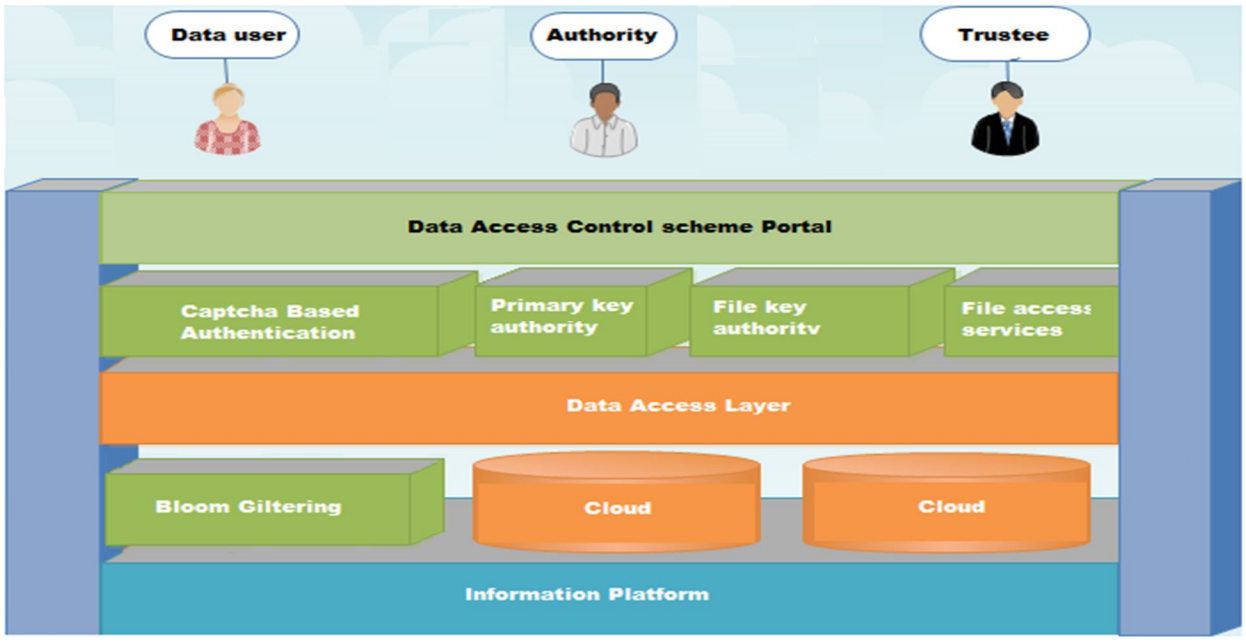
The most common type of CAPTCHA is the text CAPTCHA, which require the uses of view a destroyed string of alphanumeric character in an attached from text CAPTCHA are also rendered as MP3 audio recordings to meets the needs of visually impaired. Just as with images, both can detect the presence of an audio file but only a human can listen and know the information the file contains.

Mediated cryptography was 1st introduced traditional approach says as method to allow immediate revocation of public key. The basic idea of mediator is referred to a SEM (Security Mediator) since provides a control of security capability. The SEM does not cooperate them no transactions with public key are possible any longer.

The general idea of key insulated security was to store long terms key in a physically secure but computationally limited device short team secret keys are kept by uses on a powerful but insecure device where cryptographic computations take place.

One the key has been updated the signing or decryption algorithm does not require the device any more within the same time period. Traditional account / password based authentication is not privacy it is well acknowledged that privacy is an essential factor that must be considered in cloud computing systems. Access without secret key the adversary tries to access the system without any secret key it can have its own security devices.

System Architcture



A. Captcha Login

In this modules user having authentication and security to access the details which is presented in this image system.

B. Captcha In Authentification

In this module we use both captcha and password in a user authentication protocol which we call CAPTCHA- based password authentication (CBPA) protocol. The CBPA protocol in requires solving a captcha challenge after inputting a valid pair of user ID and password unless a valid browser cookie is received.

C. Bloom Filtering

The bloom filtering is a probabilistic space-efficient data structure that lets accurately query whether an element doesn't exist in a data set. What this means that is the bloom filter tells you that an element is not in a data set, it does so with absolute certainty.
The main aim of these modules is to check whether a given element belongs to a particular set. The bloom filter query algorithm computer all the hash value to get K array position.

II. LITERATIRE SURVEY

In this paper [1] talks about big data becomes it can mine new knowledge for economic growth and technical innovation has recently received considerable attention and many research efforts have been directed to big data processing due t its high volume, velocity and variety it referred 3V challenges.
The flourishing of big data also hinges on fully understanding and managing newly arising security and privacy challenges. If data are not authentic, new mined knowledge will be unconvincing; if privacy is not well addressed people may be reluctant to share their data. An efficient and privacy preserving cosine similarity computing protocol as an example in response to data mining's efficiency and privacy requirements in the big data era.
In this paper [2] talks about present new methodology for realizing Ciphers text - Policy Attribute Encryption (CPABE) under concrete and non-interactive cryptography assumptions in the standard model. Our solutions allows any encrypt or to specify access control in terms of any access formula over the attributes in the system. In our most efficient systems ciphers text size, encryptions and decryptions time scales linearly with complexity of the access formula the only previous work achieve these parameters was limited to a proof in the generic group model.
We present three construction within our framework first systems is proven selectively secure under a assumption that we call the [PBDHE] and other two are [BDHE] and [BDHA].
In this paper [3] talks about an attribute based encryption schema [ABE] is a cryptographic prim time in which every user is identified by set of attributes and some function of these attributed is used to determine the ability to decrypt each ciphers text this paper presents a threshold multi authority fuzzy identity based encryption [MAFIBE] scheme without a central authority for the first time an encryption an encrypt a message such that a user could only decrypt if he has at least K of the given attributes about the message.
The proposed MA-FIBE cloud be extended to the threshold multi-authority attribute based encryption.
In this paper [4] propose attribute - based encryption schemes where encryption specified access structure called ciphers text policies re hidden this will rove security of our construction based on the decisional Bilinear Diffie - Helleman assumption and the information about structure associated with the encrypted data more than the fact this are decision lines assumption.
In this paper [5] talks about new public key primitive attribute based encryption (ABE) is envisioned to be a promising tool for implementing first grained access control.
To further address the concern of user access privacy, privacy - aware ABE schemes are being developed to achieved hidden access policy recently for the purpose of secure access control there is however still one critical functionality missing in the existing
ABE schemes which is users accountability.
To improving the state of the art of anonymous CP-ABE to obtain shooter public parameter and ciphers text length. In the proposed CP- ABBE construction user accountability can be achieved in black- box model by embedding additional user specific information into the attribute private key issued to the uses while still maintain hidden access policy.

Comparative Analysis

Author Name	Method	Outcome	Demerits
R.LU, H.zhu and J.Shao [1]	Big data using (3v) high volume velocity and variety	86%	Some time accuracy will be loss Low over all performance
Brent waters [2]	CPABE PBDHE PDHE	92%	Improve to obtained more representative features
H.Lin, Z.Cao and J.Shao [3]	ABE MA-ABE	97.5%	Low error rate
T.Nishide, K.Yoneyama [4]	Decisional Bilinear Diffie -Hellman assumption	93%	Less training data set
J.Li, K.Ren , B.Zhu	ABE CP-ABBE	95.5%	Iterative training producer

III. PROPOSED SYSTEM

In this paper talks about a fine grained two factor big data access control protocol for web based cloud computing services and using captcha - Captcha and ciphers text - policy attribute - based encryption (CA-ABE) we are use two authentication systems and encrypt their data under the access policies defined over some attributed of data consumers and only allows data consumers whose attributed satisfy the access policies to decrypt the data. The device has thw following properties [1] it can compute some light weight algorithm, eg: hashing and exponentiation and [2] it is tamper resistant ie, it is assumed that no one can break into get the secret information stored inside capability it is capable of evaluation of harsh function in addition it can generate ranclom numbers and computer exponentiations of a cyclic group defined over a finite

filed ZFA access control system has been identified to not only enable the cloud severs to restrict the access to those users with the same set of attribute but also preserve user privacy.

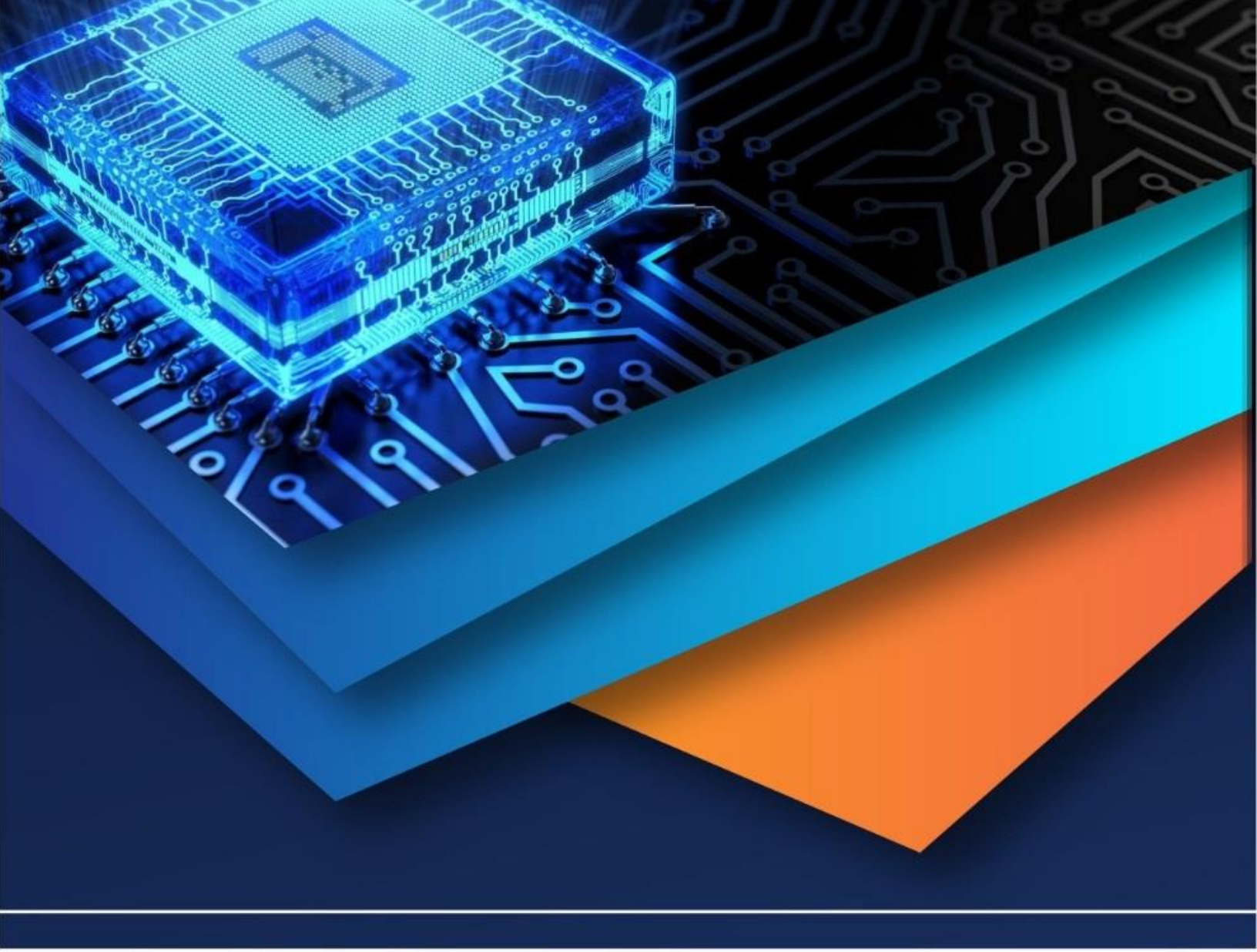
IV. CONCLUSION

This paper proposed an efficient and fine grained data access control scheme for big data where the access policy will not leak any privacy information. The ext based also designed an attribute localization algorithm is in the access policy moreover it implemented the ABF by using murmur hash and access control scheme to show that a scheme can preserve the privacy from any LSSS access policy without employing much overhead.

REFERENCE

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” [Recommendations of the National Institute of Standards and TechnologySpecial Publication 800-145], 2011.
[2] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, “Toward efficient and privacy-preserving computing in big data era,” IEEE Network, vol. 28, no. 4, pp. 46–50, 2014.
[3] K. Yang and X. Jia, “Expressive, efficient, and revocable data accesscontrol for multi-authority cloud storage,” IEEE Trans. Parallel Distrib.Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.
[4] H. Li, D. Liu, K. Alharbi, S. Zhang, and X. Lin, “Enabling fine-grained access control with efficient attribute revocation and policy updating in smart grid,” KSII Transactions on Internet and Information Systems (TIIS), vol. 9, no. 4, pp. 1404–1423, 2015
[5] K. Yang, Z. Liu, X. Jia, and X. S. Shen, “Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach,” IEEE Trans. on Multimedia (to appear), February 2016.
[6] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. of PKC’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.
[7] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” in Proc. Of INDOCRYPT’08. Springer, 2008, pp. 426–436.
[8] T. Nishide, K. Yoneyama, and K. Ohta, “Attribute-based encryption with partially hidden encryptor-specified access structures,” in Appliedcryptography and network security. Springer, 2008, pp. 111–129.
[9] J. Li, K. Ren, B. Zhu, and Z. Wan, “Privacy-aware attribute-based encryption with user accountability,” in Information Security. Springer, 2009, pp. 347–362.
[10] D. Boneh and B. Waters, “Conjunctive, subset, and range queries onencrypted data,” in Theory of cryptography. Springer, 2007, pp. 535–55
[11] J. Katz, A. Sahai, and B. Waters, “Predicate encryption supportingdisjunctions, polynomial equations, and inner products,” in Advances in Cryptology–EUROCRYPT’08. Springer, 2008, pp. 146–162.
[12] J. Lai, R. H. Deng, and Y. Li, “Fully secure cipertext-policy hiding cpabe,” in Information Security Practice and Experience. Springer, 2011, pp. 24–39

[13] L. Lei, Z. Zhong, K. Zheng, J. Chen, and H. Meng, "Challenges onwireless heterogeneous networks for mobile cloud computing," IEEE Wireless Communications, vol. 20, no. 3, pp. 34–44, 2013.
[14] K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, and W. Xiang, "Big data-driven optimization for mobile networks toward 5g," IEEE Network, vol. 30, no. 1, pp. 44–51, 2016.
[15] Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: a qoeoriented framework," IEEE Network, vol. 30, no. 1, pp. 52–57, 2016.
[16] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when qoe meets qop," IEEE Wireless Communications, vol. 22, no. 4, pp. 74–80, 2015.
[17] H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Trans. on Dependable and Secure Computing [DOI: 10.1109/TDSC.2015.2406704], 2015.
[18] K. Frikken, M. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," IEEE Trans. on Computers,vol. 55, no. 10, pp. 1259–1270, 2006.
[19] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Secure Network Protocols (NPSec'08 Workshop).IEEE, 2008, pp. 39–44.
[20] J. Lai, R. H. Deng, and Y. Li, "Expressive cp-abe with partially hidden access structures," in Proc. of ASIACCS'12. ACM, 2012, pp. 18–19.
[21] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib.Syst., vol. 24, no. 11, pp. 2171–2180, 2013.
[22] A. Beimel, "Secure schemes for secret sharing and key distribution,"Ph.D. dissertation, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[23] B. H. Bloom, "Space/time trade-offs in hash coding with allowableerrors," Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970
[24] K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec 2015.
[25] C. Dong, L. Chen, and Z. Wen, "When private set intersection meets big data: an efficient and scalable protocol," in Proc. of CCS'13. ACM, 2013, pp. 789–800.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY