INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING

IJMTARC – VOLUME – V – ISSUE – 22, APR - JUNE, 2018

ISSN: 2320-1363

AUDIT-FREE CLOUD STORAGE VIA RANDOMIZED KEY PROTOCOL

Ms M Rajya Lakshmi

Student of MCA department, Lakkireddy Bali Reddy College of Engineering, Mylavaram, Krishna district, AP.

Abstract—Cloud computing is a rising technology which provider an assortment of opportunities for online distribution of income or services. The most efficient benefit of using cloud computing is higher ease of use of services with fee and simple scalability. While the storage space of communal data on remote servers is not a new growth, current development of cloud computing validates a additional careful look at its real consequences involving privacy and privacy issues. As users no longer in fact have the storage space of their data, customary cryptographic primitives intended for the cause of data protection cannot be in a as the crow flies line conventional. In particular, just downloading all the data for its honesty confirmation is not a sensible explanation due to the expensiveness in I/O and broadcast cost across the network. As well, it is often not sufficient to detect the data dishonesty only when contact the data, as it does not present users correctness pledge for those un-accessed in order and might be too late to get well the data loss or injure. To fully make sure the data honesty and save the blur users' calculation resources as well as online load, it is of critical significance to allow public auditing repair for cloud data, so that users may option to an independent third party assessor (TPA) to audit the agreement out data when needed. The TPA, who has know-how and abilities that users do not, can rarely check the genuineness of all the data stored in the cloud on behalf of the users, which provides a much more improved and reasonable way for the user to ensure their storage appropriateness in the cloud. In a word, allowing public audit services will play an significant role for this up-and-coming cloud market to turn out to be fully recognized; where users will require ways to assess risk and gain hope in the cloud.

Keywords: Randomized key protocol, Attribute-Based Encryption, Cloud Storage, cipher text.

I. INTRODUCTION:

Cloud computing is a model for enable convenient, on-demand system access to a shared pool of configurable computing resources that can be quickly provisioned and released with negligible management effort or service supplier interaction. Another potential benefit is that in order may be better protected in the cloud. Principally, while there are benefits, present are privacy and security concerns too. The present system is based on Deniable Attribute Based Encryption system where encryption and decryption method is used. Deniable encryption involves senders and receivers creating powerful false proof of false data in code texts such that exterior coercers are satisfied. The quality based encryption uses an excellence for the key that is generated. We create use of this idea, such that cloud storage space providers can provide audit-free storage space services. In the cloud storage situation, data owners who stock up their data on the cloud are just like senders in the deniable encryption system. Persons who can access the encrypted in arrange play the role of earphone in the deniable encryption scheme, counting the cloud storage space, space providers themselves, who have system wide secrets and have to be able to decrypt all encrypted data [1]. In our move toward, the key distributor generates a unique key for the folder to the user who has right of entry to the appreciated files. When a user tries to right of admission the file which has not been allowable for that user, the cloud management marks him as the assailant. Thus maintain privacy and safety at high standards.

II. EXISTING SYSTEM:

Security is most vital part of cloud computing. Cloud computing faces a lot of of the same threats as the mental workplace. The existing systems that were used previous to fuzzy-Identity Based Encryption, Fine grained right of entry manage and Cipher text Attribute Based Encryption. In fuzzy individuality Based Encryption, A Fuzzy IBE scheme uses a confidential key for an independence, A, to decrypt a cipher text encrypted with an individuality, B, if and only if the identity A and B are close to each other as deliberate by the “set overlap” distance metric. Therefore, this scheme allows for a certain amount of error-tolerance in the identities. This idea of Fuzzy Identity Based Encryption, which allows for error-tolerance flanked by the identity of a secret key and the public key used to encrypt a cipher text. However the fuzzy reason is effectual, it has some cons. This system provide the user with an audited file, making it efficiency by auditing the files and data that has been uploaded onto the cloud server. This reduce the safety level of the scheme. In this system the basic building does not use the random oracles and provide public access to the data proprietor. It gives access to only the selected ID. In the current system, i.e Deniable Attribute-based Encryption uses the encryption method which has a variety of attributes tagged with the key generate. The hackers can decide the type of key used for solitude of data’s in the cloud. These keys are limited in length and thus can be strong-minded by diverse combination. This is a obstruction for the security of the data’s over the server. To conquer this problem of security, we propose a scheme where a single key will be generate for each user and information that will be uploaded on the cloud server.

III. PROPOSED METHODOLOGY

At present everyone opts for cloud storage space as it provides high normal of security and storage room. Right now, there are many algorithms and encryption schemes in practice. The most often used methods are fuzzy logic, Attribute Based Encryption using community finite key. But this does not give security at high standards; the use of public key will allow user to get the data of additional users. To conquer this con of the obtainable system, we move for the use of the randomized key protocol. Here the line of attack is, when the data proprietor uploads the data, it in a straight line gets stored in the cloud server. When the user wants to get back the file or data, he wants for a secret key. The Key distributor generates the key for each file on the cloud server. This key is sole for each user. When a user tries to get the information of other user, the cloud management will mark them as the hacker and will chunk the correct of entry for so as to user. Thus, preventing illegal access by the users. We suggest this system to be highly secured since of the use of the Randomized key. The key generated will be an infinite key, i.e. there is no finite length for the key. The length of the key can be customized often, making it hard to get the combination. This is the reason that this method is difficult to hack. The algorithm used in this system is the "Blowfish" algorithm. We go for this algorithm because it supports all types of file extension.

IV. ALGORITHMS

Encryption/decryption algorithm--blowfish: Blowfish is a symmetric chunk cipher algorithm for encryption/decryption. Blowfish is conventional as a fast and physically powerful encryption algorithm since it has not been cracked. In our future system we use this algorithm because, it can be used for records with diverse extensions. Since we opt for the chance key generation, it will be extremely secured since the hackers cannot predict the kind of algorithm used for the encryption procedure. The advantages of blowfish algorithm are that it is safe and easy to put into practice and most excellent for hardware completion.

V. ARCHITECTURE DIAGRAM

There are four modules; Data owner, Key admin, Cloud admin, Users. The key admin is the one which generates the sole key for each user's data on the server. When the data proprietor uploads the file it will be encrypted and can be accessed only by as long as the secret
key.

Source from Internet

VI. MODULE DESCRIPTIONS The a variety of modules developed in our proposed method involves the following:

- Data Owner
- Key Distributor
- Cloud Admin
- Users

Data Owner: Data Owner uploads records to group users via Cloud storage space like Drop box. If proprietor Upload a file in background that the file will be encrypted by Blowfish Cryptography and corroboration the Time based one time code word and enter in to cloud storage space.

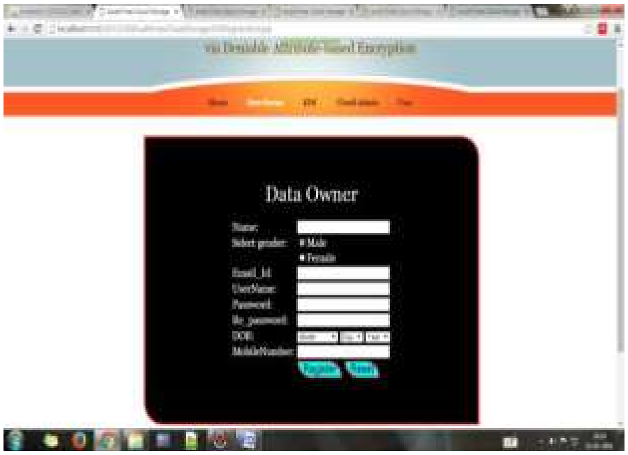


Figure 2: Data Owner

Key Distributor: Key dispenser send all the files decrypt key as well as the secret key to the users audits all the files present in cloud storage space and check the users status , file rank and aggressor status in our request.

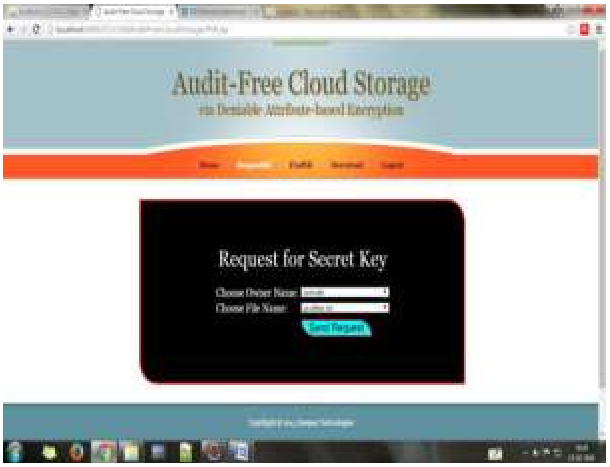
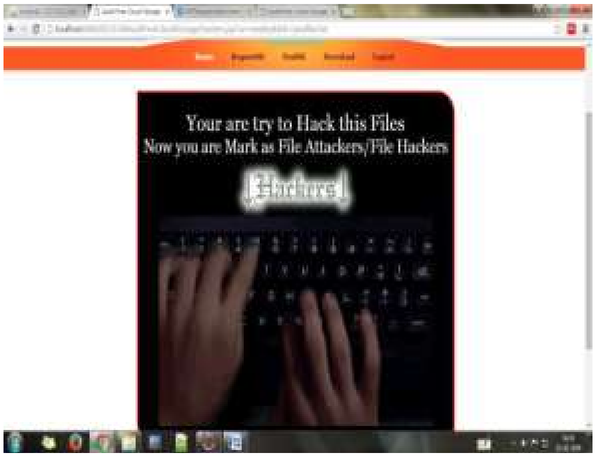


Figure 3: Requesting Secret Key Cloud Admin:

Cloud Admin confirm the Auditor endorse files following grant the final endorsement and sends that files to third party auditor and endorse users and track hackers after block the hackers in our request. Here the cloud admin will block the along with the particulars of the hacker.



Your are try to Hack this Files
Now you are Mark as File Attackers/File Hackers

Figure 4: Cloud Admin Tracking Hacker

Users: Users list first, after login he must link any group. Each and Every collection name is Unique inside the same group. User sign in the compilation login after download all records and not like this collection he will revoke the group association easily. Each and Every Users activity is tracked by Session track Methodology. If the users try to hack the one more users group name and sign in the group login that time the user system configuration & the Users Details are intimated to cloud admin. Admin chunk the hack users after the user ordinary username & password are leaving to invalid mode.

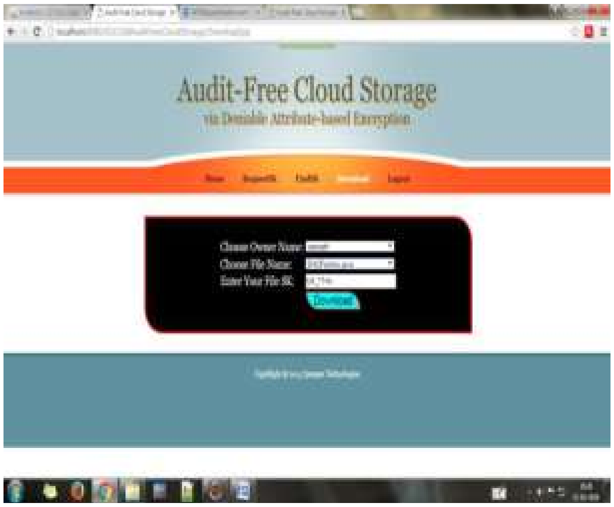


Figure 5: User Providing Secret Key

VII. EXPERIMENTAL RESULTS

Accessing the cloud server via randomized key protocol is extremely secured. In the randomized key algorithm, the sole key generated by the key distributor provides safety to the users. This method uses an audit gratis storage, which skips the third party audit of the in order and files so as to has been uploaded onto the cloud server. The key generated varies for each file and for each user. This proposed protocol is thus highly secured compared to the existing system.

VIII. CONCLUSIONS

In this proposed method, we provide an review free cloud storage which is extremely secured for the users access the cloud server using the randomized key procedure. This method makes compulsion invalid. Our future scheme provides a likely way to fight next to immoral meddling with the right of solitude.

IX. REFERENCES

[1] Po-Wen Chi, Chin-Laung Lei, "Audit-Free Cloud Storage via Deniable Attribute-based Encryption", IEEE Transactions on Cloud Computing, , no. 1, pp. 1, PrePrints PrePrints, doi:10.1109/TCC.2015.2424882.

[2] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Eurocrypt, 2005, pp. 457–473.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[5] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography, 2011, pp. 53–70.

[6] A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in Crypto, 2012, pp. 199–217.

[7] S. Hohenberger and B. Waters, “Attribute-based encryption with fast decryption,” in Public Key Cryptography, 2013, pp. 162–179.

[8] P. K. Tysowski and M. A. Hasan, “Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds.” IEEE T. Cloud Computing, pp. 172–186, 2013.

[9] Wired. (2014) Spam suspect uses google docs; fbi happy. [Online]. Available: http://www.wired.com/2010/04/cloud-warrant/
[9] Wikipedia. (2014) Global surveillance disclosures (2013present). [Online]. Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present)

[10] (2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden.

[11] (2014) Lavabit. [Online]. Available: http://en.wikipedia. org/wiki/Lavabit