ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

A Review on Key Aggregate Cryptosystem of Vital Data Distribution in Cloud

B Thejaswini[1], N Sakthi Priya[2]

ME Student , Dept of CSE, Bharath University, 173, Agaram Road, Selaiyur, Chennai, India[1].

Assistant Professor, Dept of CSE, Bharath University, 173, Agaram Road, Selaiyur, Chennai, India[2].

ABSTRACT: Emerging new computing technology cloud offers storage services. Data sharing with others in secure and efficient manner is important function in cloud storage. For this the new expandable public-key cryptosystems which derives fixed-size ciphertexts. Using expandable public-key cryptosystems transform the multiple keys of the classes as single secret key. The generated single secret key sent to others or be stored in a smart card with very limited secure storage. If a user needs to classify his ciphertexts into more than n classes, user can register for additional key pairs. Each class is indexed by a two-level index and the number of classes is increased by n for each added key. For the approach, at most two aggregate keys are needed. This key extension approach can also be seen as a key update process. In case a secret value is compromised, user can replace compromised publickey with new publickey. Eventually the approach is flexible and effective.

KEY WORDS*:* Aggregate Keys, ciphertext, Public Key Cryptosystem.

I. INTRODUCTION

Nowadays, many large scale and small scale organizations outsource their large-scale data storage to the cloud for saving the cost in maintaining their storage. With cloud storage service, the members of an organization can share data with other members easily by uploading their data to the cloud. Examples of organizations which may benefit from this cloud storage and sharing service are numerous, such as international enterprises with many employees around the world, collaborative web application providers with a large user base, or institutions dealing with big data, healthcare researchers, patients, etc. While the economic benefits brought by outsourcing data can be attractive, security is one of the most significant factors that hinder its wide development. Since data operations in the cloud are not transparent to users, and security breaches or improper practices are common and inevitable, users still have a huge concern about the security of their data on the cloud, especially on data integrity.

Cryptography is the method of storing and transmitting data in a form that only those intended for it can read and process the required data. It is technique of protecting information by encrypting the data it into an unreadable format using some encryption algorithm. Cryptography is an effective way of protecting sensitive information that is to be stored on media or transmitted through network communication paths. The main goal of cryptography is that to hide information from unauthorized individuals like intruders or hackers. Hackers now a day can hack most of the cryptography algorithms and the information can be revealed if the attacker has enough time and resources to hack the data. So a more realistic goal of cryptography is to decrypting the data to be difficult.

Considering data privacy, rely on the server to enforce the access control after authentication, if there is any unexpected privilege escalation will

expose all data which is sensitive. In a shared- cloud computing environment, things become even worse because Data from different clients can be hosted on separate virtual machines (VMs) but reside on a single physical machine. Regarding availability of files, there is lot of cryptographic schemes which allows a third-party auditor to check the availability of files on behalf of the data owner without leaking anything about the data, or without compromising the data owner's anonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

II. RELATED WORK

Key Aggregate Cryptosystem

Sharing data or information among users is an important functionality in cloud storage. In this paper [1] Proposed new public-key cryptosystems that produce constant-size ciphertexts. The one can aggregate any set of secret keys and make them as compact as a single key, but the power of all the keys being aggregated. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. How to a decryption key more powerful in the sense that it allows decryption of multiple ciphertexts, without increasing its size. A different type of public key encryption "key aggregate cryptosystem" in which the users inscribe a data using an identifier of ciphertext called class which means the ciphertexts are further categorized into different classes. The key data owner of the data holds a master-secret key, to extract secret keys for different classes of the ciphertext from the cloud . Implementation of the KAC system in C with the pairing-based cryptography (PBC) Library.

Remote data checking protocols using provable data possession

In this paper[3] a framework for provable data possession. A PDP protocol checks that associate degree outsourced storage website retains a file, that consists of f blocks. The data owner preprocesses the file, generating a tiny low piece of data that's keep domestically, transmits the file to the server S, and should delete its native copy. The server stores the file and responds to challenges issued by the consumer. As a part of preprocessing, the consumer could alter the file to be kept at the server. The consumer could encipher, encode, or expand the file, or could embody further data to be keep at the server. Before deleting its native copy of the file, the consumer could execute a data possession challenge to form certain the server has with success keep the file.

Aggregate and Verifiably Encrypted Signatures from bilinear Maps

In this paper[4] The conception of aggregate signatures and an efficient aggregate signature theme supported bilinear maps. Key generation, aggregation, and verification need no interaction. Construct an aggregate signature theme supported a recent short signature because of Boneh, Lynn, and Shacham (BLS). This signature theme works in any cluster wherever the decision Diffie- Hellman problem (DDH) is straightforward; however the procedure Diffie-Hellman problem (CDH) is difficult.

For security, introduced the extra constraint that associate degree aggregation signature is valid on condition that it's an aggregation of signatures on distinct messages. The constraints are often satisfied by prepending the general public key to the message before language. Aggregate signature theme offers verifiably encrypted signatures. Aggregate signatures square measure helpful for reducing the dimensions of certificate chains (by aggregating all signatures within the chain) and for reducing message size in secures routing protocols like SBGP.

Multi-Authority Attribute-Based Encryption

In this paper[5] Attribute based encryption (ABE) determines decoding ability supported a user's attributes in an exceedingly multi-authority ABE theme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decoding keys to users and encryptors will need that a user acquire keys for applicable attributes from every authority before decrypting a message. Multi-authority ABE theme exploitation the ideas of a trustworthy central authority (CA) and global identifiers (GID). The CA has the facility to decode each ciphertext that appears somehow contradictory to the initial goal of distributing management over several probably untrusted authorities. The use of an identical GID allowed the authorities to mix their data to create a full profile with all of a user's attributes that unnecessarily compromises the privacy of the user.

Proxy Re-encryption scheme

In this paper, end users on client machines would like to get access to integrity-protected, confidential content. A content owner publishes encrypted content within the kind of a many-reader, single- writer file system. The owner

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

encrypts blocks of content with distinctive, bilaterally symmetrical content keys. A content secret's then encrypted with associate degree uneven master key to create a lockbox. The lockbox present within the block it protects.

Untrusted block stores create the encrypted content out there to everybody. Users transfer the encrypted content from a block store, then communicate with associate degree access management server to decipher the lockboxes protective the content. The content owner selects that users ought to have access to the content and offers the acceptable delegation rights to the access management server.

once a certified user requests access to a file, the access management server uses proxy re-encryption to directly re-encrypt the acceptable content key(s) from the master public key to the user's public key.

Public Auditability and Data Dynamics for Storage Security in Cloud Computing

In this paper[7] explored the matter of providing cooccurring public auditability and data dynamics for remote data integrity check in Cloud Computing. to attain efficient data dynamics, improved the prevailing proof of storage models by manipulating the classic Merkle Hash Tree (MHT) construction for block tag authentication. To support efficient handling of multiple auditing tasks, more explore the technique of additive aggregate signature to increase main result into a multi-user setting, wherever TPA will perform multiple auditing tasks at the same time. in depth security and performance analysis show that the projected theme is extremely efficient and incontrovertibly secure.

To effectively support public auditability while not having to retrieve the information blocks themselves, resort to the homomorphic appraiser technique. Homomorphic authenticators are unforgeable data generated from individual data blocks, which may be firmly aggregate in such the way to assure a verifier that a linear combination of data blocks is properly computed by confirmatory solely the aggregate appraiser. In our style, we tend to propose to use PKC based mostly homomorphic appraiser to equip the verification protocol with public auditability.

Provable Data Possession at Untrusted Server

In this paper[8] Provable data possession (PDP) that permits a client that has hold on data at associate degree untrusted server to verify that the server possesses the initial information while not retrieving it. The model produces probabilistic proofs of possession by sampling random sets of blocks from the server that drastically reduces I/O prices. Key parts of projected schemes are the homomorphic verifiable tags. PDP enable verificatory information possession while not having access to the particular information file. Obvious information possession (PDP) that gives probabilistic proof that a third party stores a file.

The model is exclusive in this it permits the server to access tiny parts of the file in generating the proof; all different techniques should access the whole file. at intervals this model, given the first provably-secure theme for remote data checking. PDP schemes give info independence that may be a relevant feature in sensible deployments and place no restriction on the quantity of times the client will challenge the server to prove data possession. Also, main PDP theme offers public verifiability.

Privacy-Preserving Audit

In this paper [9] present protocols that permit a third- party auditor to sporadically verify the info hold on by a service and assist in returning the info intact to the client. most significantly, protocols are privacy-preserving, in this they ne'er reveal the info contents to the auditor. The answer removes the burden of verification from the client, alleviates each the customer's and storage service's worry of knowledge run, and provides a technique for freelance arbitration of knowledge retention contracts. Associate in nursing auditor will intercede knowledge retention contracts between storage provider and client. Protocol has 3 phases: initialization, audit, and extraction.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Proofs of Retrievability for Large Files

A POR scheme allows an archive or back-up service (prover) to supply a apothegmatic proof that a user (verifier) will retrieve a target file F, that is, that the archive retains and dependably transmits file information sufficient for the user to recover F in its totality. A POR is also viewed as a sort of scientific discipline proof of data (POK), however one specially designed to handle an oversized file (or bit string) F. Authors explored POR protocols here within which the communication prices, range of memory accesses for the prover, and storage needs of the user (verifier) are little parameters basically freelance of the length of F. In a POR, in contrast to a POK, neither the prover nor the verifier would like even have data of F. PORs as a crucial tool for semi-trusted on-line archives.

III. ISSUE IN CURRENT ENVIRONMENT

Data sharing is an important functionality in cloud storage. For example, bloggers can let their friends view a subset of their private pictures; an enterprise may grant her employees access to a portion of sensitive data. The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. Users should be able to delegate the access rights of the sharing data to others so that they can access these data from the server directly. However, finding an efficient and secure way to share partial data in cloud storage is not trivial. Clouds are still facing the broad range of both internal and external threats for data integrity, security of the encryption and the other the privacy of the users.

IV. PROPOSED METHOD

The EKAC Scheme

The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via KeyGen. Using KeyGen can extend the Public key and aggregate key. Messages can be encrypted via Encrypt by anyone who also decides what ciphertext class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of ciphertext classes via Extract. The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any ciphertext provided that the ciphertext's class is contained in the aggregate key via Decrypt.

The EKAC Scheme consists of six polynomial time algorithm as follows:

1. Setup(1λ,n):executed by the data owner to setup an account on an untrusted server.on input a security level parameter 1λ and the number of ciphertext class n,it putputs the public system parameter param.

2. KeyGeneration:executed by the data owner to randomly generate a public/master-secret key pair(pk,msk).

3. Extend(pkl ,mskl): Execute keyGen() to get(vl+1 , ϒl+1) Є G×Zp ,output the extended public and master secret keys aspkl+1 =(pkl ,vl+1),mskl+1 =(mskl, ϒl+1).

4.Encryption (pk, i, m) :It is executed by data owner and for message m and index i ,it computes the ciphertext as C.

5..Extraction (msk, S): It is executed by data owner for delegating the decrypting power for a certain set of ciphertext classes and it
outputs the aggregate key for set S denoted by Ks.

6. Decryption (Ks, S, I, C): It is executed by a delegate who received, an aggregate key Ks generated by Extract. On input Ks, set S, an index i denoting the ciphertext class ciphertext C belongs to and output is decrypted result m.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

The EKAC polynomial algorithm uses MD5 encryption algorithm for encryption and decryption.

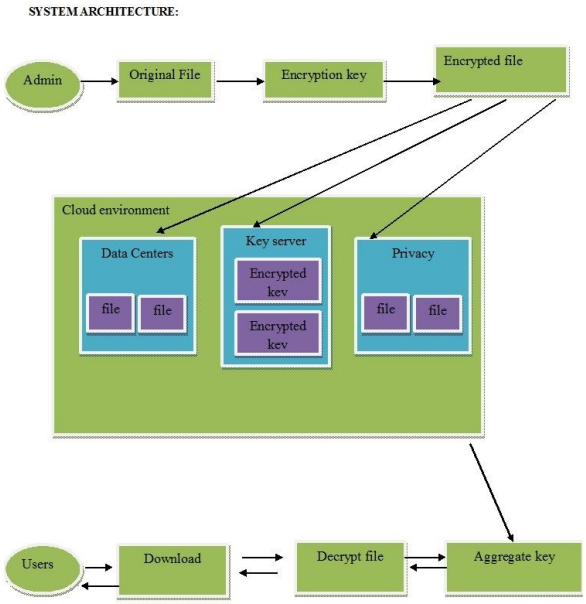

Figure 1: System Architecture of EKAC

V. EXPERIMENTAL RESULTS

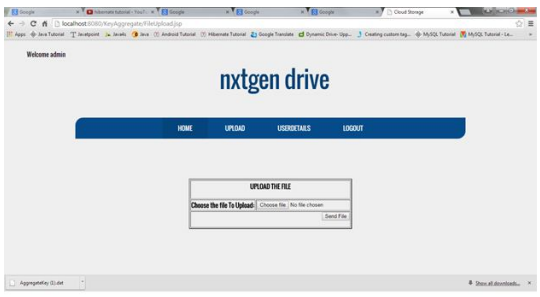

Figure 2: Admin uploads the required file to the requested user

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

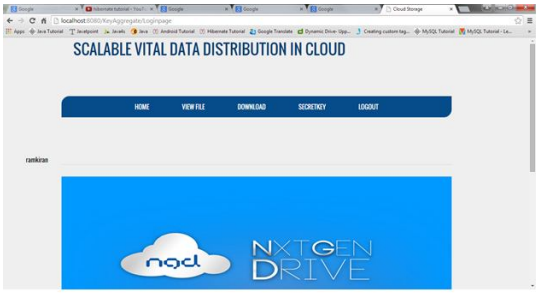

Figure 3: user can view the list of files send by the admin

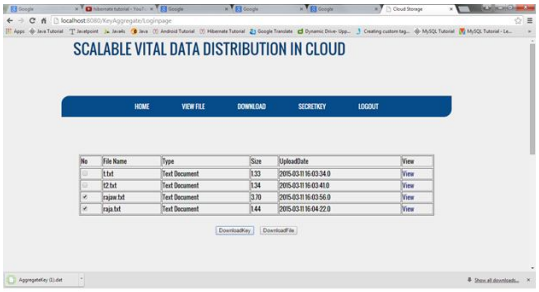

Figure 4: The user can select the list of files and download the file/files using aggregate key

Above Figures shows the results of fig 2 :the admin can share the required files that are needed by the user and fig 3 shows that the user can view the list of file and the user can select the files for downloading. Fig 4 specifies that the user can download the selected files in the form of zip file.

VI. CONCLUSION

How to protect user's data privacy is a central question of cloud storage. The fundamental idea of the approach is to focus on how to "compress" secret keys in public-key cryptosystems and also need to expand the public-key, if a user needs to classify his ciphertexts into more than n classes, user can register for additional key pairs. Each class now is indexed by a two-level index and the number of classes is increased by n for each added key. For the approach, at most two aggregate keys are needed .

REFERENCES

1. Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H," Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" , IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014.
2. Cloud Storage "IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.
3. Reza Curtmola and Osama Khan Randal Burns, "Robust Remote Data Checking" , Proceedings of the 4th ACM international workshop on Storage security and survivability PAGES63-68 ACM 978-1-60558-299-3.
4. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps", Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.
5. Melissa Chase and Sherman S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", Pages 121-130 ACM New York, NY, USA ©2009 978-1-60558-894-0.
6. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.
7. Qian Wang , Kui Ren, Wenjing Lou and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", Parallel and Distributed Systems, IEEE Transactions on Volume:22 , Issue: 5 Page(s):847 – 859.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

8. Giuseppe Ateniese , Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner ,Zachary Peterson and Dawn Song, "Provable Data Possession at Untrusted Stores", Proceeding CCS '07 Proceedings of the 14th ACM conference on Computer and communications security Pages 598-609.
9. Mehul A. Shah Ram Swaminathan and Mary Baker, " Privacy-Preserving Audit and Extraction of Digital Contents", HP Labs Technical Report No. HPL-2008-32.
10. Ari Juels1 and Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files" , Proceeding CCS '07 Proceedings of the 14th ACM conference on Computer and communications security Pages 584-597.

BIOGRAPHY

B.Thejaswini received the B.E degree in Computer Science and Engineering from Sri Chandrashekarendra Saraswathi Viswa Maha Vidyalaya in 2011. Completed .Net certified course in 2011. Worked as Programmer Analyst in CTS, Chennai from 2011 to 2013. Pursing M.Tech Computer Science and Engineering from Bharath University. Participated in workshops on getting started with Android, .Net C# WPF and PHP and How to build a software.

M.Sakthi Priya received B.E degree from Perunthalaivar Kamarajar Institute of Engineering and Technology (PKIET) Karaikal, India and M-Tech in 2011-2013 from the Pondicherry University. She is working as an Assistant professor at Bharath University for last two years. She has published over 7 research papers in international and national journals of repute.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015