ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Survey on Aggregate Cryptosystem for Scalable Vital Data Distribution in Cloud Storage

B. Thejaswini[1], M.Sakthi Priya[2]

Dept of CSE, Bharath University, 173, Agaram Road, Selaiyur, Chennai, India[1,2].

ABSTRACT: Cloud computing technology is widely used so that the data can be outsourced on cloud can accessed easily. Different users can share that data through different virtual machines which present on single physical machine. But the thing is user don't have control over the outsourced data. The main purpose is to share data securely among users. The cloud service provider and users Authentication is necessary to make sure no loss or leak of users data in cloud. Privacy preserving in cloud is important. Cryptography helps the data owner to share the data to the requested user in safe way. For that the data owner encrypts the data and uploads on server. The encryption and decryption keys may be different or same for different set of data. For decrypting the required data only the set of decryption keys are shared. Here a public key cryptosystems which generates a ciphertext which is of constant size. The difference is one can collect a set of secret keys and make them as small size as a single key with holding the same ability of all the keys that are formed in a group as aggregate key.

KEYWORDS: Cloud storage, Attribute base encryption, Identity base encryption, Cloud storage, data sharing, key aggregate encryption

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'sanonymity. Likewise, cloud users probably will not hold the strong belief that the cloud server is doing a good job in terms of confidentiality.

The layout of the paper is as follows. In section II, address the above mentioned techniques and also give a brief on the literature being reviewed for the same. Section III, presents a comparative study of the various research works explored in the previous section. Section IV, describes about future work. Section V gives the conclusion in and lastly provides references.

II. RELATED WORK

Sharing data or information among users is an important functionality in cloud storage. In [1] author Proposed new public-key cryptosystems that produce constant-size ciphertexts such that efficient delegations of decryption rights for any set of ciphertexts are possible. 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. More important is that the extracted key can be an aggregate key which is as condense as a secret key for a single class, but combines the power of many such keys that is the decryption power for any subset of ciphertext classes. Implementation of the KAC system in C with the pairing-based cryptography (PBC) Library.

In[2] authorsspecialize in a privacy-preserving public auditing system for information storage security in cloud computing. privacy-preserving public auditing theme uses the homomorphic linear critic and random masking to ensure that the third -party administrator wouldn't learn any dataregardingthe information content hold on the cloud server throughout the economical auditing method, that not solely eliminates the burden of cloud user from the tedious and presumablycostly auditing task, howeverconjointly overcome the users worry of their externalization informationoutpouring. The framework assumes that the TPA is homelessthat's TPA doesn'thave to maintain and update state between audits, thatcould be a main property requiredwithin the public auditing system. A public auditing theme consists of 4 algorithms (KeyGen, SigGen, GenProof, VerifyProof). KeyGencould be a key generation rulethat'spass by the user to setup the theme. SigGenis employed by the user to get verification data, which cancomprises digital signatures. GenProof is pass by the cloud server to getan indicationof information storage correctness, whereasVerifyProof is pass by the TPA to audit the proof.Considering TPA couldat the same time handle multiple audit sessions from completely different users for his or her outsourced information files, [2] additional extend privacy protective public auditing protocol into a multiuser setting, wherever the TPA will perform multiple auditing tasks during a batch method for higherpotency. in depth analysis shows that planned schemes area unitdemonstrably secure and extremelyeconomical. Preliminary experiment conducted on Amazon EC2 instance additional demonstrates the quick performance of plannedstyle on each the cloud and therefore the auditor aspect.

In [3]authors provide a framework for provable datapossession. A PDP protocol (Figure1) checks that associate degree outsourced storage website retains a file that consists of f blocks. The consumer C (data owner) preprocesses the file, generating a tiny low pieceof datathat'skeepdomestically, transmits the file to the serverS,and should delete its native copy. The server stores the file and responds to challenges issued by the consumer. Storage at the server is Ω (f) and storage at the consumer is O (1), orthodox to our notion of associate degree outsourced storage relationship. As a part of preprocessing, the consumercould alter the file to be kept at the server. The consumercouldencipher, encode, or expand the file, or couldembodyfurtherdata to be keep at the server. Before deleting its native copy of the file, the consumercould executea data possession challenge to formcertain the server has with successkeep the file.

In[4] authors produces 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.The security of the system during this model that offers the opponent selection of public keys and messages to forge. For security, introduced the extra constraint that associate degree mixture signature is valid on condition that it's an aggregation of signatures on distinct messages. This constraint is satisfied naturally for the applications. 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.

In[5] authors proposed Attribute based encryption (ABE)which 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 willneed that a user acquire keys for applicable attributes from every authority before decrypting a message. Multi-authority ABE themeexploitation the ideas of a trustworthy central authority (CA) and world identifiers (GID). However, the CA in this construction has the facility to decodeeach ciphertext that appears somehow contradictory to the initial goal of distributing management over severalprobably untrusted authorities. The use of an identical GID allowed the authorities to mix their datato create a full profile with all of a user’s attributes that unnecessarily compromises the privacy of the user. Resolutionthat removes the trustworthy central authority, and protects the users’ privacy by preventing the authorities from pooling their data on explicit users.

In [6] 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 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, and 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. Access management victimization Proxy Cryptography. Associate degree improvement on the access management server model that reduces the server’s trust needs by victimization proxy cryptography. during this approach, the content keys accustomed cypher files square measure themselves firmly encrypted below a master public key, employing a simplex proxy re-encryption theme of the shape delineated during this work. as a result of the access management server doesn't possess the corresponding secret key, it can't be corrupted therefore on gain access to the content keys necessary to access encrypted files. The key master secret key remains offline, within the care of a content owner who uses it solely to get the re-encryption keys employed by 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.

In [7] authors explored the matter of providing co-occurring 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.

In [8] authors proposed 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.

In [9] authorspresent a protocols that permit a third- party auditor to sporadically verify the infohold 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 worryof knowledgerun, and provides a technique for freelance arbitration of knowledge retention contracts. Associate in nursing auditor willintercedeknowledge retention contracts between storage provider and client. Protocol has 3 phases: initialization, audit, and extraction.

In [10] authors provide POR schemeallowsan 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) arelittle parameters basicallyfreelance of the length of F. In a POR, in contrast to a POK, neither the prover nor the verifier would likeeven havedata of F. PORs as a crucial tool for semi-trusted on-line archives.

III. COMPARATIVE STUDY

In this section analyzed the various research works on several parameters and presented their comparison in the table below.

Table 1: COMPARISON OF VARIOUS RESEARCH WORKS

S.No	Title	Author	Issue	Method Used	Tools	Advantage	Disadvantage
1.	Privacy-Preserving Public Auditing for Secure Cloud Storage	Cong Wang Sherman S.M. Chow Kui Ren,	Users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing	Privacy preserving Public auditing protocol method	C and cloud server side in Amazon Elastic Computing Cloud (EC2)	scheme enables an external auditor to audit user’s cloud data without learning the data content.	CSP might hidedata loss incidents to maintain a reputation
2.	Robust Remote Data Checking	Reza Curtmola Osama Khan	The integration of Forward Error Correction (FEC) codes with remote data checking schemes that	the forward error-correcting encoding method	Monte-Carlo simulation model-C++	Protection against corruption of a large portion of File. Theclient will detect with high	These data checking protocols are asymptotically less efficient

			rely on spot checking			probability if the server corrupts more than a -fraction of file.	
3.	Aggregate and Variably Encrypted Signatures from Bilinear Maps	Dan Boneh Craig Gentry Ben Lynn HovavShacham	signature constructions using generic gap Diffie-Hellman group	aggregate signatures with bilinear maps	Java	Aggregate signatures usefulfor reducing the size of certicate chains and for reducing message size in secure routing protocols	security of the system in a model that gives the adversary choice of public keys and messages to forget.
4.	Improving Privacy and Security in Multi-Authority Attribute-Based Encryption	Melissa Chase Sherman S.M. Chow	the trusted centralauthority, GIDcompromises the privacy of the user	Attribute Based Encryption Scheme	Java	Removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users,	In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption Keys to users.
5.	Chosen-Ciphertext Secure Proxy Re-Encryption	Ran Canetti Susan Hohenbergery	Re-encryption scheme achieved only semantic security. IN contrast, applications often require security against chosen ciphertext attacks.	Proxy re-encryption scheme using Decisional Bilinear Diffie-Hellman(CCA-secure PRE)	Proxyenabled Chefs file system	PRE schemes that are secure in arbitrary protocol settings, Or in other words are secure against chosen ciphertext attacks.	It is often not sufficient to guarantee security in General protocol settings.
6.	Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed	Giuseppe Ateniese Kevin Fu	BBS Scheme which is transitive and bi-directional	proxy re-encryption technique	Chefs database is encrypted with a 128-bit AES content key in	Re-encryption schemes that realize a stronger notion of security, and the usefulness of proxy re-encryption	In this only a limited amount of trust is placed in the proxy and proxy re-encryption to achieve CCA2 security in a multi-user

	Storage				CBC mode	method of adding access control to a secure file system.	setting.
7.	Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing	Qian Wang Cong Wang	TPA-ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations	Third party auditor and merikle hash tree	linux	Public auditability for storage correctness assurance.	Do not address the issue of data privacy
8.	Provable Data Possession at Untrusted Stores	Giuseppe Ateniese Randal Burns	weaker guarantee by enforcing storage complexity	Provable Data Possession (E-PDP)	Linux	The PDP model for remote data checking supports large datasets in widely distributed storage systems.overhead of server is low	It provide a weaker guarantee by enforcing storage complexity:
9.	Privacy-Preserving Audit and Extraction of Digital Contents	Mehul A. Shah Ram Swaminathan	privacy preserving auditing and extraction of digital contents	Encrypted Key Extraction using Modified version	Java	protocols are privacy-preserving, in that never reveal the data contents to the auditor	There are no fair and explicit mechanisms for making the services accountable for data loss
10.	PORs: Proofs of Retrievability for Large Files	Bedford Hopkinton	cryptographic proof of knowledge (POK), donot verify that archives do not delete or modify files prior to retrieval	Proof of retrivability method	Java	The goal of a POR is to accomplish the checks without users having to download the filesthemselves and quality-of-service guarantees	This imposes some computational overheadbeyond that of simple encryption or hashingas well as larger storage requirements on the prover

IV.FUTURE WORK

The case study was very useful to understand the techniques. It is well understood that how the techniques are used to share the data in cloud securely.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

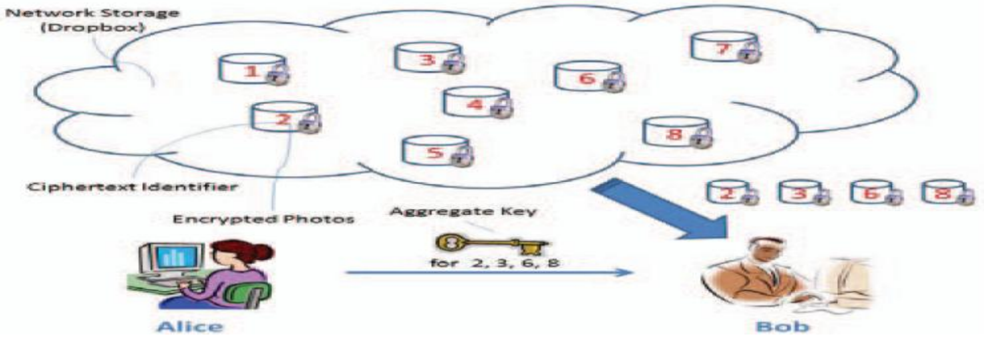

fig 1: Data Sharing in cloud

The aggregate key encryption combined with ciphertext, which prevent attacks with high security. Key distribution can be managed easily with perfect security. The access policy and cryptographic schemes are getting more versatile and often involve multiple keys for a single application. Approach is more flexible than other key assignment which can only save a data.

V.CONCLUSION

In this paper, literature survey on key aggregate cryptosystem was helpfulto grasp the technique and the way the techniques area unit developed to share knowledge among users in cloud. To share knowledge flexibly is importantfactor in cloud computing. Users like to transfertheirknowledge on cloud and among totally different users. Outsourcing of knowledge to server could lead to leak the personalknowledge of user to everybody. Codingcould be a one solution that provides to share selected knowledge with desired candidate. Sharing of cryptography keys in secure method plays vital role. Public -key cryptosystems provides delegation of secret keys for totally different ciphertext categories in cloud storage. The delegate gets firmlyassociatecombination key of constant size. It'sneeded to keep enough range of cipher texts categories as they increase quick and the ciphertext categoriesarea unitfinitethat's the limitation.

REFERENCES

1. Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, 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.
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.
6. 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.
7. 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.
8. Mehul A. Shah Ram Swaminathan and Mary Baker, " Privacy-Preserving Audit and Extraction of Digital Contents",HP Labs Technical Report No. HPL-2008-32.
9. 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

1. B.Thejaswini received the B.E degree in Computer Science and Engineering from Sri ChandrashekarendraSaraswathiViswaMahaVidyalaya 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.

2. M.SakthiPriya 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 nationaljournals of repute.