IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Group Data Sharing in Cloud Computing on Identity Based Encryption

N Babu[1],M.E, Ph.D. **M Sonali[2] D Venkatesh[3] K Subba Reddy[4] V Saikumar[5]**

[1]Assistant Professor, [2345]UG Student [12345]Department of Computer Science and Engineering,

[12345]Siddharth Institute Of Engineering & Technology, Tirupathi, Andhra Pradesh, India.

ABSTRACT

One of the most popular ways to protect data secrecy in many real-world applications, such as cloud-based data storage systems, is using encryption technologies. However, the production of encrypted data in a largely "static" format may obstruct further data processing. For computation or other purposes, encrypted data might need to be "converted" into another format. The idea of encryptions witching was first put up for conversion, namely between Paillier and ElGamal encryptions, in order to allow encryption to be employed in another device equipped with a different encryption mechanism. The conversion between traditional identity-based and attribute-based encryptions is taken into consideration in this research, and it also makes a concrete construction suggestion using the proxy re-encryption technique. In the standard model, it is demonstrated that the design is CPA secure under the q-decisional parallel bilinear Diffie-Hellman exponent assumption. The performance comparisons show that, especially when the client's data is encrypted and outsourced to a distant cloud, our bridging technique lowers compute and communication costs on the client side. In practise, it is acceptable to incur the computational overhead associated with re-encryption (on the server side) and decryption (on the client side).

INDEX TERMS: *CPA security, identity-based encryption, attribute-based encryption, encryption switching, data security.*

INTRODUCTION

These days, cloud garage is becoming more well-known. We observe an increase in demand for records outsourcing in organisational settings, which helps with the strategic management of corporate information. Also, it serves as an intermediate period at the base of a lot of web services for personal applications. These days, using it is straightforward and cost-freefor email photo albums, document sharing, and/or remote access, with storage sizes more than 25GB (or some bucks for more than 1TB). Thanks to the cutting-edge Wi-Fi age, users may access practically all of their documents and emails using a mobile phone from any location in the world. When it comes to maintaining information privacy, a conventional method is to rely on the server to implement the obtain entry to manage after authentication; nevertheless, this exposes all information to any unanticipated privilege escalation. Things get worse in a shared-tenancy cloud computing environment. Records from specific clients can live on a single physical body but be hosted on several virtual machines (VMs).

LITERATURE SURVEY

Cryptography & Encryption

The foundation of the cybersecurity sector is cryptography and encryption. In this section of the blog, you will learn about the various applications of cryptography and how encryption is a part of everything we do online. Some of the terms you will frequently hear in the industry include AES, DES, and RSA.

Secret Sharing

refers to cryptographic techniques for dividing a secret into several shares and giving each share to a different party, with the goal of preventing the secret from being revealed until all the shares are brought together. The person who is in possession of a secret, often known as the dealer, a secret is divided into n shares, and a threshold t is established for the number of shares needed to reconstruct the secret. The dealer then distributes the shares such that they are held by various parties.

An adversary who obtains access to fewer shares of the secret than the threshold cannot learn the secret in safe secret sharing techniques. Because they enable more secure storage of highly sensitive data, such as encryption keys, missile launch codes, and digitised bank accounts, secret sharing systems are beneficial. The data is dispersed so that there isn't a single point of failure that could cause it to be lost. The use of software-based methods to generate a high level of security for secrets makes secret sharing schemes crucial in cloud computing environments (as opposed to requiring specialised hardware).

IBE, or identity-based encryption An essential ID-based cryptography primitive is identity-based encryption (IBE). As a result, it is a sort of public-key encryption where a user's public key is some distinctive information about their identity (for instance, an email address). The text-value of the recipient's name or email address, for example, could be used as a key to encrypt a message by a sender who has access to the system's public parameters. A centralised authority provides the receiver with its decryption key, which must

Identity-based encryption uses a trusted third-party server to generate the appropriate private key from the public key after the user generates the public key from a known unique identifier (such as an email address). This eliminates the requirement for distributing public keys before sharing encrypted data. The recipient's unique identifier can be used by the sender to create a public key and encrypt the contents. With the aid of the private-key generator, a dependable third-party server, the receiver is able to create the appropriate private key (PKG). The PKG first releases a master public key and then keeps the associated master private key in order to use this encryption method (referred to as master key). Each party can calculate a public key corresponding to an identity given the master public key by fusing the master public key with a known identity value (i.e. an email address). The owner of the identity that produced the public key contacts the PKG to request a corresponding private key, and the PKG creates the private key using its master private key.

IBE is advantageous because it does not call for the pre-distribution of public keys (referred to as certificates in PKI). On the other hand, it needs a reliable outsider—the PKG.

RECENT WORKS

Compact key in symmetric key encryption: The owner of the facts uses a master key to encrypt his data before uploading them to a cloud server.

Everyone who wants to share those statistics wants to have access to the same master decryption key.

Keys for a Predefined Hierarchy in Cryptography

It reduces the cost of handling and storing secret keys.It creates a tree-like structure. When a department is given a key, the keys of its descendant nodes are derived using the same key.

LIMITATIONS

• Forget that rekeying is necessary after revocation.

• The saved files are need to undergo re-encryption.

• intricate modular arithmetic procedures.

• More hidden keys are created.

• Drives up the price of storing and

• Sending the textual content of the cipher

PROPOSED METHOD

In this research, we investigate how to increase the efficiency of a decryption key without increasing its size so that it can decipher several cypher texts. Our challenge is to create a green public-key encryption scheme that supports flexible delegation in the sense that any subset of the cypher texts created by the encryption scheme is decrypted using a regular-length decryption key that is generated by the owner of the master-secret key. Our solution to this problem is the introduction of a unique type of public-key encryption that we call key-combination cryptosystem (KAC). Customers encrypt messages in KAC not only using a public key, but also using a cypher text identification known as elegance. Meaning that the cypher texts are also divided into special training. The key owner is in possession of a grasp-mystery key, a master-secret that may be utilised to extract mystery keys for exclusive classes. More significantly, the extracted key can be a combined key that is as small as a mystery key for a single elegance but aggregates the power of several such keys, that is, the decryption power for any subset of cypher text content classes. This user secret key is supplied to users, who can use it to decrypt messages that have been encrypted using the master key.

Advantages of Proposed system:

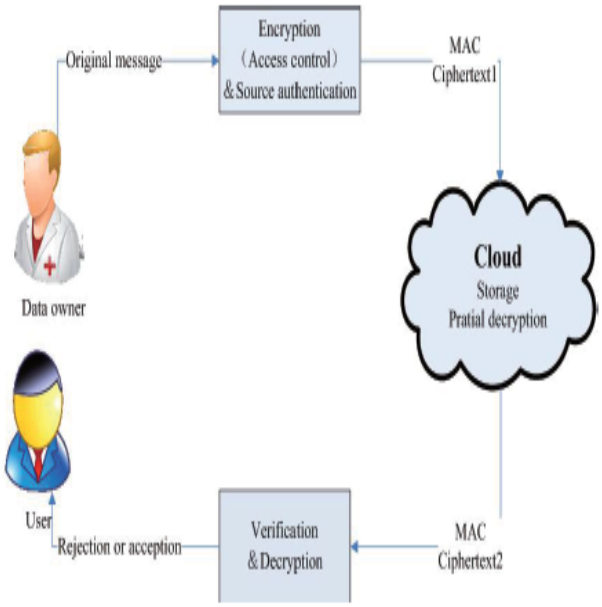
The key that was extracted could be a tiny combo key that opens only one door with style.

Identification-based encryption

The aggregate key can be used to implement the delegation of decryption properly.

The Administrator can quickly identify changes in the planned system.

Architecture Diagram



ALGORITHM:

CSD Algorithm:

Input:
GMem-> Group Member
GMan-> Group Manager
CS-> Cloud Server

Output:
Result->R
Step 1: GMem register, login and upload files
Step 2: GMem view files which uploaded
Step 3: GMem-> (req.) GMkey from GMan
Step 4: GMan generates key ->GMem
Step 5: GMem<-(reci.)GMankey ->(req.) CS
Step 6: CS -> (send) cloud key ->GMem
Step 7: KAC encrypt all files
Step 8: GMem access user files
Step 9: GMem decrypt files using KAC
Step 10: GMem get R

MODULES DESCRIPTION

Setup segment: Aside from the known wellbeing parameter, no further information is used in the setup computation. It produces a grip key MK and the general population characteristics PK.

Segment encryption: scrambling (PK, M, A). The message M, the inspire admission, and the general society parameters PK are entered into the encryption computation in order to shape An over the universe of characteristics. Only a client that

possesses a set of characteristics that satisfy the motivate admittance to shape will be able to decode the message, since the computation will encode M and transmit a figure content CT in this manner. We can anticipate that the figure message actually contains A.

Setup segment: Just the known wellbeing parameter is used in the setup computation. No other data is used. It generates a grip key (MK) and the characteristics of the general population (PK).

Segment encoding:

Decode (PK, CT, and SK) (PK, CT, and SK). The general population parameters PK, the figure content CT, which includes a get right of section to strategy An, and the private key SK, which is a private key for a fixed S of traits, are entered into the unscrambling computation. The calculation will decode the figure message and return a message M if the set S of properties matches the entry requirement for structure A.

EXPERIMENTS

It is necessary to consistently formalise the description of information security threats, resources, assessments of the level of information security, options (types) of measures to ensure information security, and selection of the best (rational) option from them in order to formalise the process of ensuring information security in library information systems. There is a collection that contains every scenario that could arise when assessing the availability and quality of information resources. The terms of access to resources (passwords, online, on a computer, in a local network, etc.), the conditions for resource storage, the price of the resource (determined by experts, a membership fee, or other means), the amount of information, the type of document, etc. a collection of all potential dangers to information resources. The set, which contains numerous measures to It is a subsystem and only contains the conditions for the status and assessment of information resources unique to a certain object (library, Fund, etc.). In actuality, it describes a certain circumstance. a subset of risks that relate to a certain circumstance; a subset of safeguards to assure information security in the event of risks to a particular circumstance. Information security requires both the identification of potential dangers to a specific situation and the selection of the most effective countermeasures (Actions) (Threats). The complexity of the issue stems from the nondeterministic nature of the correspondences between set elements. Finding the correspondences between the sets and formalising the solution in accordance with them is the task that is most challenging in practise. Existing deterministic methods used to try to tackle the issue are unsuccessful.

CONCLUSION & FUTUREWORK

A concentrated investigation of distributed storage is the most efficient way to guarantee the security of clients' personal information. Cryptographic schemes are becoming more flexible and frequently contain many keys for a single application as we develop more scientific tools. In this article, we look at how to "pack" mystery keys in open key cryptosystems to support the distribution of mystery keys for various cypher text classes. The delegate can easily obtain a total key of a constant size regardless of whatever class is chosen from the force set of classes. Compared to other tiered key tasks, which can only free up spaces if every keyholder uses a similar arrangement of keys, our solution is more flexible. The specified bound of the number of most severe cypher text classes serves as a restriction in our work. The quantity of cypher texts frequently grows quickly in distributed storage. Hence, in order to prepare for future expansion, we must save enough cypher text classes. If not, we must develop people generally as we have shown.

BIBLOGRAPHY

1] S. S. M. Chow, Y. J. He, L. C. K. Hue, and S.-M. You, "SPICE -Simple Privacy-Preserving Identity Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.

[2] L. Hardesty, "Secure computers aren't so secure," MIT press, 2009, http://www.physorg.com/news176107396.html.

[3] C. Wang, S. S. M. Chow, Q. Wang, K. Reno, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[5] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.

[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.

[7] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[8] J. Beano, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.

[9] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.