Policy Based Broadcast Access Authorization In Cloud

Dr R Pushpalakshmi[1], Priyadarshini M[2]
[1, 2] Dept of Information Technology
[1, 2] PSNA College of Engineering and technology, Dindigul, Tamilnadu

Abstract- *Cloud storage services enable data owners to send cipher text versions of potentially sensitive material (such as private genetic data) to faraway cloud servers.*

Many proxy re-encryption (PRE) techniques have been developed to allow data owners to share data encrypted in cipher texts further. Most systems, however, only offer single-recipient or coarse-grained re-encryption, which may limit data sharing flexibility. We propose a Policy-based Broadcast Access Authorization (PBAA) approach to overcome this problem by including the well-known identity-based broadcast encryption (IBBE) and key-policy attribute-based encryption into PRE. A data owner can use IBBE to encrypt his data for a group of recipients under our PBAA scheme. More crucially, the data owner can create a delegation key with an access policy and transmit it to the cloud, which will convert any initial cipher text that meets the access policy into a new cipher text for a new set of receivers. Cloud users can exchange their remote data in a secure and flexible manner with these functionalities.

The PBAA system is both secure and efficient, according to security and performance evaluations.

Cloud computing, data sharing, proxy re-encryption, and broadcast encryption are all terms that can be found in the index.

I. INTRODUCTION

Cloud computing has evolved from a daring notion to widespread use across a variety of application fields. The intricacy of the technology that underpins cloud computing, on the other hand, creates new security concerns and challenges. Threats and mitigation approaches for the IaaS model have been closely scrutinized in recent years, with the industry investing in better security solutions and issuing best practice recommendations. From the perspective of the end user, cloud infrastructure security involves complete faith in the cloud provider, which is sometimes backed up by reports from external auditors. While providers may provide security upgrades such as data encryption in transit, end-users have little or no control over these methods. For enterprises that rely on cloud infrastructure, there is an obvious need for practical and cost-effective cloud platform security solutions. Platform integrity verification for compute hosts that support virtualized cloud infrastructure is one such approach. Several prominent cloud suppliers have indicated that this approach will be implemented in the near future, with the goal of protecting cloud infrastructure from insider attacks and advanced persistent threats. In terms of these implementations, we observe two key improvement vectors. For starters, the specifics of such exclusive solutions aren't made public, so they can't be implemented or improved by other cloud platforms. Second, none of the solutions, to our knowledge, offer cloud tenants with assurance of the integrity of compute hosts that support their slice of the cloud infrastructure. To address this, we propose a set of protocols for trusted launch of virtual machines (VM) in IaaS, which provide tenants with a proof that the requested VM instances were launched on a host with an expected software stack. we propose a Policy-based Broadcast Access Authorization (PBAA) scheme by introducing the well-established identity-based broadcast encryption (IBBE) and key-policy attribute-based encryption into PRE. To enable data owners to further share the data encrypted in cipher texts, In a secure and flexible way Security analysis and performance evaluation show that the PBAA scheme is secure and efficient, respectively.

Proxy re-encryption (PRE[5]) would be a good way to solve the problem of exchanging encrypted data. A proxy (e.g., the cloud) with some required information (a.k.a. re-encryption key) can convert a cipher text intended for Alice into a new cipher text for Bob in PRE. Identity-based PRE (IBPRE [6]) inherits all of the benefits of PRE while also allowing any recognized string to serve as a public key, removing the burden of managing public keys in standard PRE systems. IBPRE has been widely employed in various practical applications such as cloud data sharing [6], [7], [8], e-mail forwarding [9], online social networks [10], and micro-video subscribing systems [11] due to its attractive features.

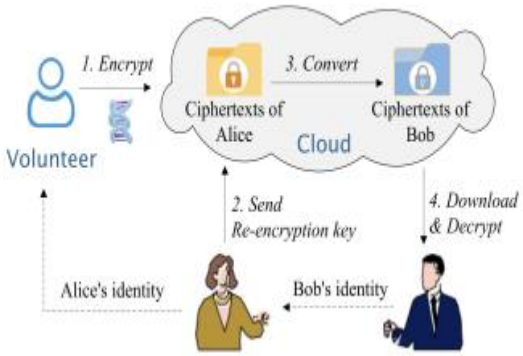


Figure 1 IBPRE

Figure 1 shows how IBPRE is used to share data in the cloud. Assume there are people who are willing to share their own genetic data for medical study. To collect and share genetic data, the cloud is used. A volunteer encrypts his data before outsourcing it to prevent it from being viewed by unauthorized people or the cloud

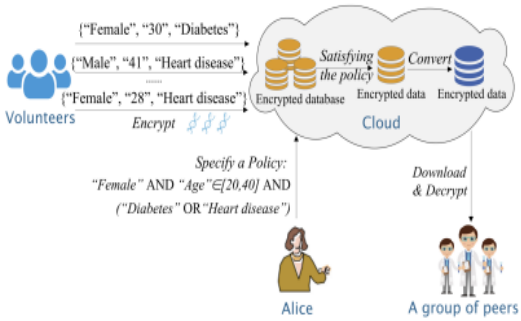


Figure 2:data sharing in cloud

With IBPRE, the volunteer utilizes the researcher Alice's identity to encrypt the genome data so that only Alice has access to it. Alice may, at some moment, If we like to share the genome data with a colleague (Bob) in order to collaborate on a project. Thanks to IBPRE's re-encryption process, Alice can generate a re-encryption key based on Bob's identity and distribute it This is the cloud's key. The cipher texts can then be converted via the cloud. Meant for Alice into Bob's cipher texts When you go online, Bob can decrypt the cipher texts by downloading them from the cloud. Using his own key, he decrypted the genetic data.

IBPRE enables ciphertext conversion from one recipient to another, allowing data to be shared across several users.

IBPRE does, however, have some restrictions. In particular, Alice can only share encrypted data with one recipient at a time in IBPRE. If Alice wants to share data with more people, she'll have to generate a re-encryption key for each of them, which will cost a lot of time and effort. Furthermore, IBPRE only allows for "all-or-nothing" data sharing, which means Alice can either give all of her data or none at all. Because of these restrictions, IBPRE would be unsuitable for some more complex applications. Consider the following situation to further explain this notion. Assume that Alice has access to the encrypted genome data that has been provided by various volunteers. Before uploading the genome data, volunteers annotated it with descriptive tags, such as "Female", "Age"=30, and "Diabetes" to indicate that the genome data belonged to a 30-year-old lady with hereditary diabetes. Alice would like to share some genetic data with a group of colleagues in order to collaborate on a project. For example, Alice wants to exchange the genome data of 20-40 year old women with diabetes or heart disease, i.e. data whose tags fit the following criteria: "Female" AND "Age" [20, 40] AND ("Diabetes" OR "Heart Disease") (see Fig. 2). The peers cannot directly access the genome data because it has already been encrypted.

As a result, Alice may require a flexible re-encryption process that may convert encrypted genome material that satisfies the access policy into cipher texts that the group of peers can decrypt.

Because of its single receiver and "all-or-nothing" data sharing limits, IBPRE isn't a good fit for this case. To address the "all-or-nothing" problem, Shao et al. devised the identity-based conditional PRE (IBCPRE [12]), in which Alice can set a condition for a re-encryption key, allowing the proxy to only convert encrypted data that matches the condition. Unfortunately, IBCPRE does not enable multiple conditions to be specified in a re-encryption key, therefore Alice will have to generate multiple re-encryption keys if she needs to specify many conditions for the purpose of data sharing .Furthermore, IBCPRE only allows for single-recipient data sharing, therefore a group of users cannot view the data at the same time. Another option is to employ the conditional identity-based broadcast PRE (CIBPRE [9]), which allows numerous recipients to share data. However, unlike IBCPRE, CIBPRE only permits one condition to be provided in a re-encryption key, limiting data sharing flexibility.

II. OUR CONTRIBUTIONS

The verifiability of the cloud's transformation provides a mechanism to check the transformation's validity. This is not, however, formally defined as verifiability.

However, following the approach defined in the literature, it is not possible to create ABE schemes with verifiable outsourced decryption.[9]

Furthermore, the existing technique is based on random oracles (RO). Unfortunately, the RO model is heuristic, and a proof of security in the RO model does not indicate that an ABE scheme in the actual world is secure.

There are cryptographic techniques that are secure in the RO model but inherently insecure when the RO is instantiated with any real hash function, as is widely known. Many proxy re-encryption (PRE) techniques have been developed to allow data owners to disseminate data encrypted in cipher texts more widely. Most systems, however, only offer single-recipient or coarse-grained re-encryption, which may limit data sharing flexibility.

we propose a Policy-based Broadcast Access Authorization (PBAA) approach to overcome this problem by including the well-known identity-based broadcast encryption (IBBE) and key-policy attribute-based encryption into PRE. A data owner can use IBBE to encrypt his data for a group of recipients under our PBAA scheme.

More crucially, the data owner can create a delegation key with [4]an access policy and send it to the cloud, allowing the cloud to convert any initial cipher text that meets the access policy into a new cipher text for a new group of receivers.

Cloud users can exchange their remote data in a secure and flexible manner with these functionalities. The PBAA system is both secure and efficient, according to security and performance evaluations.

III. RELATED WORK

Broadcast Encryption

1. Fiat and Naor first proposed the notion of broadcast encryption [13] where a data owner can encrypt a message to a group of recipients at a time. Traditional broadcast encryption (e.g., [14], [15], [16]) relies on a third party to manage public-key certificates of all users, which would incur a singlepoint problem.
2. Then Delerablee [17] proposed the identity-based ´ broadcast encryption (IBBE) scheme that avoids the use of publickey certificates by allowing any public identities to serve as public keys.
3. Sakai and Furukawa [18] also presented an IBBE scheme with small-size cipher texts and private keys. To revoke the access rights of a recipient to a broadcast cipher text.

Identity-based proxy re-encryption.

Broadcast encryption allows for secure multi-recipient data sharing, however it is difficult to facilitate sharing encrypted data with recipients other than those who were initially chosen. In order to address this problem,

Blaze et al. proposed the concept of proxy re-encryption (PRE) [5]. In PRE, a proxy can be authorized to transform Alice's cipher texts into Bob's cipher texts, so that the encrypted data can be shared from Alice to Bob.

Later, Green and Ateniese [6] extended PRE to identitybased PRE (IBPRE), which mitigates the public-key certificate management problem.

To resist collusion attack from the proxy and the users authorized to access re-encrypted data Zhang et al. [24] presented a collusion-resistant IBPRE scheme.

Shao and Cao [25] proposed a multi-time IBPRE scheme in which a cipher text can be re-encrypted for multiple times. This multi-time IBPRE allows an authorized user to further share the re-encrypted ciphertext to others. To achieve encrypted data sharing with a group of recipients

Conditional proxy re-encryption

While it is a practical way to transfer encrypted data, (identity-based) PRE poses a privacy risk by giving the proxy too much power in the re encryption process. The proxy can convert all of a data owner's cipher texts using the re-encryption key; however, the data owner may only want to communicate a portion of cipher texts at times. To accomplish this,

Weng et al. proposed conditional PRE [27], whereby a data owner can specify a condition in the re-encryption key such that only the cipher texts satisfying the condition can be transformed by the proxy. Vivek et al. [28] enhanced the efficiency of Weng et al.'s scheme by reducing the number of bilinear pairing operations.

Chu et al. [29] proposed a conditional broadcast PRE scheme which allows to generate multi-recipient cipher texts in the conditional PRE settings

System Architecture

A central authority (CA), a cloud service provider (CSP), data owners, and data users are the four organizations that make up the PBAA system (as depicted in Fig. 3). CA is a fully trusted party in charge of releasing the system's public key and responding to data owners' and users' registration requests. CSP has a large number of resources for storage and processing. CSP, in particular, provides a storage service for data owners to store the ciphertexts of their data, as well as a compute service to re-encrypt the ciphertexts. As a result, CSP saves both original and re-encrypted ciphertexts. In real-world circumstances, a company can purchase CSP's storage and computing services and the organization's IT centre serves as the CA. Then cloud services will then be available to all CA workers who have enrolled.

Data owners can outsource their data to tpa for data sharing. Specifically, a data owner can designate a set S of identities of the intended data users and a set L of descriptive conditions (e.g., keywords of the data content), encrypting his data with these two sets. The resulting (original) cipher text is subsequently outsourced to CSP. When data users in the set S are connected to the internet, they can retrieve the cipher text from CSP and decrypt it with their private keys. If the data owner or an authorized data user in S wants to share data with a new group of users (denoted by s), the data owner creates an access structure A over conditions and then generates a delegation key (i.e., re-encryption key)

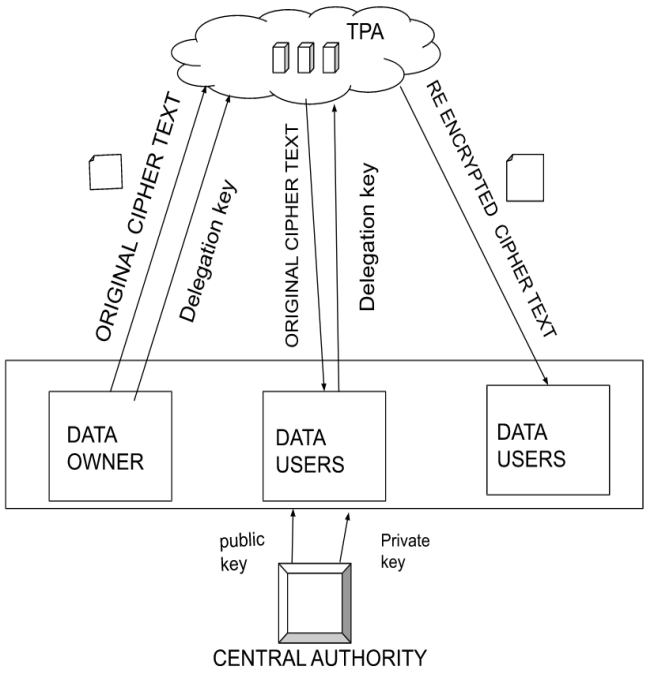


fig:3: system architecture of PBBA

Policy based access authorization architecture

using A and the identities of the users in S. CSP turns the original cipher texts with conditions satisfying the access structure into re-encrypted cipher texts that all users in s can decrypt using their own private keys using this delegation key.

IV. CONSTRUCTION

Registration

In the registration stage, CA first checks whether a user is allowed to join in the system. For example, the IT center (CA) of a company checks whether a user requesting to use the cloud services is a valid employee. If yes, CA generates a private key and sends it to the user as an authorized credential to access the data stored in the cloud. To generate a private key, CA first determines a unique identity ID for the user

Self registration and login forms are designed to create the register and login interface to the system. By using that username and password they can login into session and can send the file request to the admin.

Partition Split

User can upload file into the system. The user uploaded files are automatically splitted into three parts. The first partition file is encrypted and stored in the cloud server. Each file will have OTP Key. The third party cannot access this file without admin permission.

Send Request

The user can send request into the system. The admin will login and view user request details. The admin sends OTP Key to the user request email id.

Storage

Cooper at al described in a secure platform architecture based on a secure root of trust for grid environments – precursors of cloud computing. Trusted Computing is used as a method for dynamic trust establishment within the grid, allowing clients to verify that their data will be protected against malicious host attacks. The authors address the malicious host problem in grid environments, with three main risk factors: trust establishment, code isolation and grid middleware. The solution established a minimal trusted computing base (TCB) by introducing a security manager isolated by the hypervisor from grid services (which are in turn performed within VM instances). The secure architecture is supported by protocols

for data integrity protection, confidentiality protection and grid job attestation. In turn, these rely of client attestation of the host running the respective jobs, followed by interaction with the security manager to fulfill the goals of the respective protocols.

TPA

We now describe two protocols that constitute the core of this paper's contribution. These protocols are successively applied to deploy a cloud infrastructure providing additional user guarantees of cloud host integrity and storage security. For protocol purposes, each domain manager, secure component and trusted third party has a public/private key pair

The private key is kept secret, while the public key is shared with the community. We assume that during the initialization phase, each entity obtains a certificate via a trusted certification authority.

Encryption

A data owner can securely share data with a group of receivers using the PBAA scheme. Specifically, the data owner establishes a set S of receivers' identities.

Delegation

The data owner (or authorized user in S) can still share certain data with a new group of receivers once a volume of data has been encrypted and outsourced to the cloud. Let's say the data owner wishes to communicate information on the first quarter's turnover and development costs for an electronic device. The data owner creates an access policy first.

Decryption

When a data user gets online, he can download a cipher text from CSP and try to decrypt it using his private key. We note that there are two kinds of cipher texts stored in the cloud, i.e., original cipher texts and re-encrypted cipher texts

V. VERIFICATION & VALIDATION

Client Side Validation

Various client-side validations are employed to verify that only legitimate data is entered on the client side. Client-side validation reduces server load and saves time when dealing with invalid data.

- VBScript is used to ensure that only the appropriate data is entered into the required fields. The maximum lengths of the fields on the forms have been set correctly.• Forms cannot be submitted without the mandatory data being filled in, so that manual errors such as submitting empty mandatory fields can be handled out at the client side, saving the server time and load.
- Tab-indexes are set based on the user's needs and the simplicity with which they can work with the system.

Validation on the server

Some checks aren't possible to perform on the client side. Server-side checks are required to prevent the system from failing and informing the user that an invalid operation has been performed or that the operation done is restricted. The following are some of the server-side checks that have been implemented: A server-side restriction has been imposed to validate the validity of the main and foreign keys. It is impossible to duplicate the value of a primary key. Any attempt to duplicate the primary value generates a notice informing the user of those values. Forms using foreign keys can only be modified with the existing foreign key values.

•Various Access Control Mechanisms have been established so that one user does not agitate another through suitable alerts regarding successful activities or exceptions occurring at the server side. According to the organizational structure, access permissions for various sorts of users are managed. Only authorized users are allowed to log in and have access to the system, which is determined by their category. On the server side, user names, passwords, and permissions are managed, and server-side validation is used to put limits on a number of prohibited operations.

VI. ANALYSIS

The performance of the PBAA scheme was evaluated through a series of trials. The technique was implemented using a client/server model, with the client running on a Windows 10 PC with a Core i7 intel processor and 16 GB RAM, and the server running on an Alibaba Cloud ECS 64-bit dual core 16GB-memory Windows server. Socket and UDP protocols are used to communicate between the client and the server. The PBAA scheme is made up of bilinear groups,
and the PBC library (https://crypto.stanford.edu/pbc/) contains routines for basic group operations such group creation, exponentiation, bilinear map, and hash map.

To implement each PBAA algorithm, we used the PBC package (written in C) and the Visual studio 2010. On the PC client, we perform the system setup, registration, encryption, delegation, and decryption algorithms, while the

cloud server runs the re-encryption algorithm. We used an elliptic curve with a 160-bit group order in the simulation, which provides a comparable security level to 1024-bit RSA. For backwards compatibility, we used the concept of key encapsulation in the implementation. As a result, we encrypt real data with 128-bit AES keys before encrypting the AES keys with the PBAA's encryption technique. The medical images in the Edinburgh Dermo Fit library (https://licensing.eri.ed.ac.uk/i/software/dermofitimage-library.html) were used in the tests. Furthermore, because the PBAA model permits

Our studies were conducted with varied conditions so that we could exchange findings with multiple receivers.

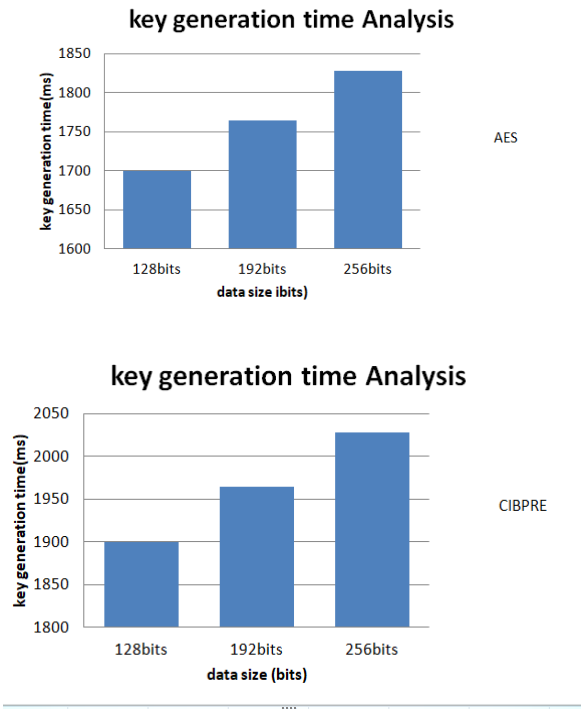


Figure4:key generation comparision analysis

the above fig1graphs depicts the key generation time analysis accordingly with regard to data bits and time in seconds here is a comparison with CIBPRE module and the proposed module

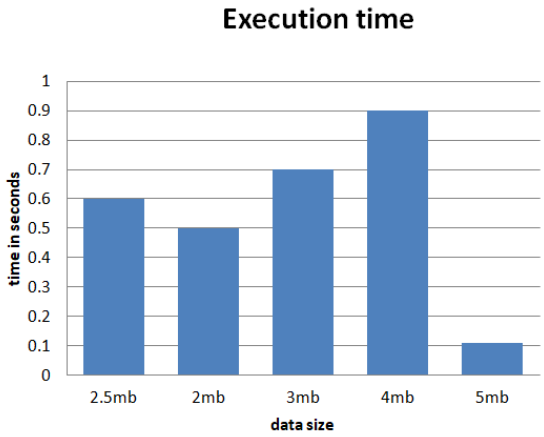


Figure 5:execution encryption time analysis

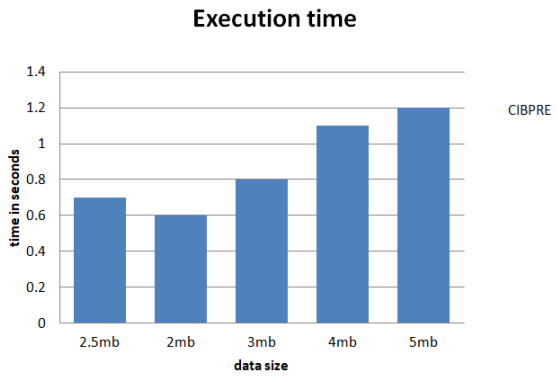
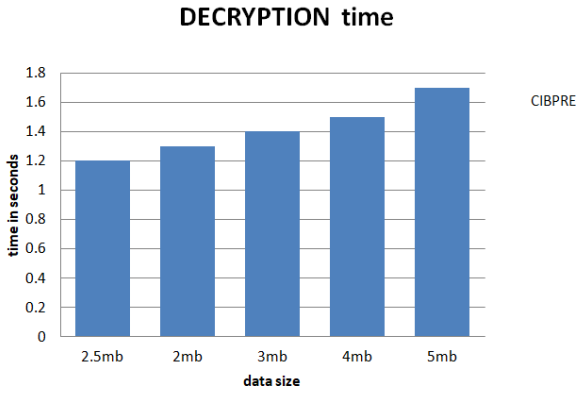
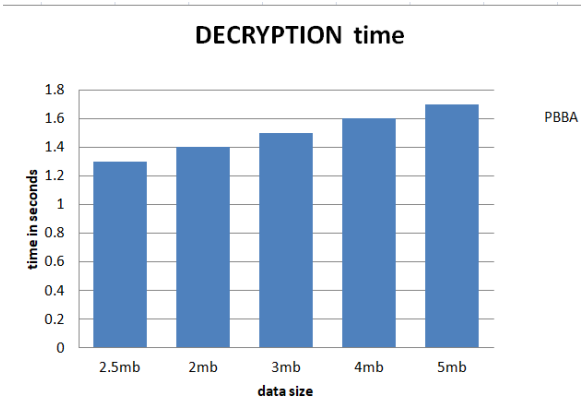


Figure 6:execution encryption time analysis

This fig 5 and fig 6 depicts the execution time for the Partitions based on their size of data the time taken to encrypt has been measured and analyzed in means of seconds





Figre7:decryption analysis

fig 7 the decryption time to show the output has been compared between the proposed PBAA with the CIBPE module the messages are decrypted and output is verified

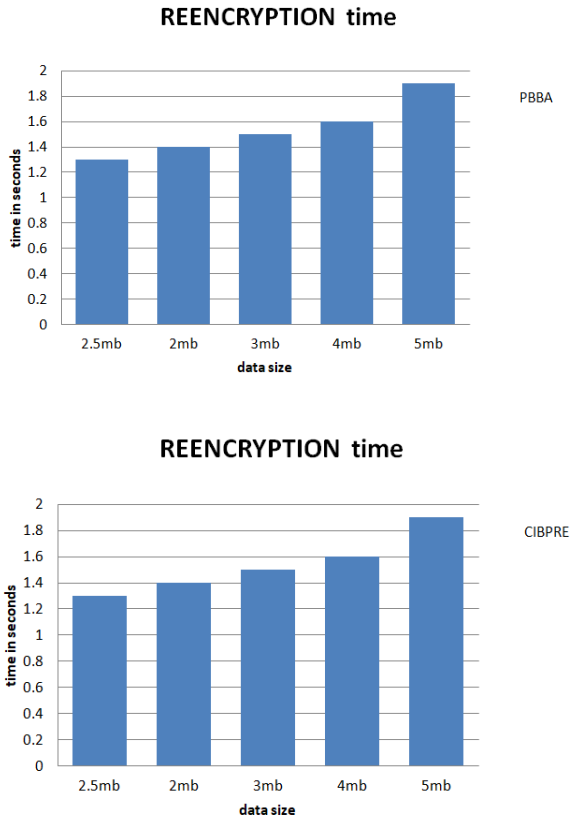


Fig8: re-encryption analysis

Figure 8 explains the comparison graph between the existing and proposed module in the means of time complexity. The above analysis reveal that PBBA scheme achieves a practicable access authorization and can be transferred to multiple users with lost cost time efficiency and security.

VII. CONCLUSION

In this paper, We looked into ways to distribute encrypted data in the cloud in a flexible way in our study. The suggested PBAA approach employs IBBE to achieve multi-recipient data sharing, as well as a fine-grained re encryption mechanism through the use of linear secret sharing.

The PBAA scheme therefore gives a flexible access authorization for data owners to distribute their encrypted data for the first time.

The data owner can, for example, produce a delegation key with an access policy and then send it to the cloud, which can then re-encrypt the encrypted data to make it accessible to a new group of receivers. The suggested technique is proven to be secure, and show that it is efficient and practical.

REFERENCES

[1] J. Srinivas, K. Reddy, and A. Qyser, “Cloud Computing Basics,” Build. Infrastruct. Cloud Secur., vol. 1, no. September 2011, pp. 3–22, 2014.

[2] M. A. Vouk, “Cloud computing - Issues, research and implementations,” Proc. Int. Conf. Inf. Technol. Interfaces, ITI, pp. 31–40, 2008.

[3] P. S. Wooley, “Identifying Cloud Computing Security Risks,” Contin. Educ., vol. 1277, no. February, 2011.

[4] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, “An Overview of Cloud Services Adoption Challenges in Higher Education Institutions,” 2015.

[5] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.

[6] F. Zhang and H. Chen, “Security-Preserving Live Migration of Virtual Machines in the Cloud,” J. Netw. Syst. Manag., pp. 562–587, 2012.

[7] J. Hu and A. Klein, “A benchmark of transparent data encryption for migration of web applications in the cloud,” 8th IEEE Int. Symp. Dependable, Auton. Secur. Comput. DASC 2009, pp. 735–740, 2009.

[8] D. Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M. and Huemer, “Retaining data control to the client in infrastructure clouds,” Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.

[9] E. Mohamed, “Enhanced data security model for cloud computing,” Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012.

[10] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at

different layers of Cloud computing," J. Supercomput., vol. 63, no. 2, pp. 561–592, 2013.

[11] C. Ge, L. Zhou, J. Xia, P. Szalachowski, and C. Su, "A secure fine-grained identity-based proxy broadcast re-encryption scheme for micro-video subscribing system in clouds," in International Symposium on Security and Privacy in Social Networks and Big Data. Springer, 2019, pp. 139–151.

[12] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in 2011 IEEE International Conference on Communications (ICC). IEEE, 2011, pp. 1–5.

[13] A. Fiat and M. Naor, "Broadcast encryption," in Annual International Cryptology Conference. Springer, 1993, pp. 480–491.

[14] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in CRYPTO 2005. Springer, 2005, pp. 258–275.

[15] D. Boneh and B. Waters, "A fully collusion resistant broadcast, trace, and revoke system," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 211–220.

[16] J. Kim, W. Susilo, M. H. Au, and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 679–693, 2015.

[17] C. Delerablee, "Identity-based broadcast encryption with constant size ´ ciphertexts and private keys," in International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2007, pp. 200–215.

[18] R. Sakai and J. Furukawa, "Identity-based broadcast encryption." IACR Cryptology ePrint Archive, vol. 2007, p. 217, 2007.

[19] J. Lai, Y. Mu, F. Guo, W. Susilo, and R. Chen, "Anonymous identitybased broadcast encryption with revocation for file sharing," in Australasian Conference on Information Security and Privacy. Springer, 2016, pp. 223–239.

[20] "Fully privacy-preserving and revocable id-based broadcast encryption for data access control in smart city," Personal and Ubiquitous Computing, vol. 21, no. 5, pp. 855–868, 2017.

[21] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in International Workshop on Public Key Cryptography. Springer, 2011, pp. 53–70.

[22] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, 2013, pp. 463–474.

[23] L. Zhang, H. Xiong, Q. Huang, J. Li, K.-K. R. Choo, and J. Li, "Cryptographic solutions for cloud storage: Challenges and research opportunities," IEEE Transactions on Services Computing, 2019.

[24] L. Zhang, H. Ma, Z. Liu, and E. Dong, "Security analysis and improvement of a collusion-resistant identity-based proxy re-encryption scheme," in International Conference on Broadband and Wireless Computing, Communication and Applications. Springer, 2016, pp. 839–846.

[25] J. Shao and Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption," Information Sciences, vol. 206, pp. 83–95, 2012.

[26] C. Ge, Z. Liu, J. Xia, and F. Liming, "Revocable identity-based broadcast proxy re-encryption for data sharing in clouds," IEEE Transactions on Dependable and Secure Computing, 2019.

[27] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009, pp. 322–332.

[28] S. S. Vivek, S. S. D. Selvi, V. Radhakishan, and C. P. Rangan, "Conditional proxy re-encryption-a more efficient construction," in International Confere