

# An Efficient Approach to Enable Hierarchical Integration of File Records onto the Cloud using FH-ABE Scheme

Dr. Shubhangi D C<sup>1</sup>, Pooja Chawan<sup>2</sup>

Associate Professor, Department of Computer Science & Engineering, VTU PG Centre, Kalaburagi, Karnataka, India<sup>1</sup>

P.G Student, Department of Computer Science & Engineering, VTU PG Centre, Kalaburagi, Karnataka, India<sup>2</sup>

**Abstract:** One of the most favored encryption innovations to tackle the testing issue of secure information partaking in distributed computing is Ciphertext-policy attribute-based encryption (CP-ABE). The shared information records for the most part have the normal for multilevel progression, especially in the region of human services and the military. In any case, CP-ABE does not investigate the hierarchy order structure of shared records. A productive record chain of importance attribute-based encryption plan is proposed in distributed computing. The layered get to structures are incorporated into a solitary get to structure, and after that, the progressive documents are scrambled with the coordinated get to structure. The ciphertext parts identified with attributes could be shared by the records. Accordingly, both ciphertext data storage and time cost of encryption are bifurcated. In addition, the proposed plan is ended up being secure under the standard presumption. Test reenactment demonstrates that the proposed plan is very proficient regarding encryption and decryption. With the quantity of the records expanding, the upsides of our plan turn out to be increasingly prominent.

**Keywords:** Ciphertext-policy, attribute-based encryption, data sharing, file hierarchy.

## I. INTRODUCTON

Cloud Computing is the utilization of processing assets (equipment and programming) that are conveyed as an administration over a system (regularly the Internet). The name originates from the normal utilization of a cloud-formed image as a reflection for the intricate foundation it contains in framework charts. It has administrations with a client's information, programming and calculation. It consists of tools and programming assets made accessible on the Internet as oversight outsider administrations. These administrations normally give access to cutting edge programming applications and top of the line systems of server PCs.

The objective of cloud computing is to apply customary supercomputing, or elite computing power, typically utilized by military and research offices, to perform several trillions of calculations for each second, in shopper arranged applications, for example, money related portfolios, to convey customized data, to give information stockpiling or to influence huge, immersive PC diversions.

The cloud computing utilizes systems of expansive gatherings of servers normally running ease shopper PC innovation with specific associations with spread information preparing errands crosswise over them. This common IT framework contains huge pools of frameworks that are connected together. Regularly, virtualization systems are utilized to augment the energy of cloud computing.

As more and more customers are making use of the information, they require some means of storage platform that keeps their data safe and intact. Cloud computing provide one such platform to do the same. It helps the users to store massive amount of information and allows the data sharing effectively. In order to prevent the data from eavesdropping or leaking, cloud computing allows the user to encrypt the data by using different means prior to the data being shared.

The first step towards the defense can be Access control which limits the unauthorized access from the shared information. In near years, a technique called Attribute-based encryption scheme has become popular as it can hold the information security and acknowledge fine-grained, one-to-numerous, and access control. One more scheme named Ciphertext-policy attribute based encryption (CP-ABE) is more efficient and can be utilized for common application aspects.

The proposed system involves different users with different roles and access level. As the files are arranged in hierarchical level of tree, each user with corresponding access control can download the file. Cloud Service Provider (CSP), is the overall care taker of the data, server, and ensure variety of services to the users. The authority center entertained the user with assigning the keys and creates some secret parameters. Data Owner uploads the file onto cloud in the encrypted form to prevent the illegal access. The User on the other hand, request for the interested file and uses

his keys to decrypt the desired ciphertext from the CSP. The files stored onto the CSP are arranged in hierarchical form. This is nothing but a collection of files divided according to some parameter kept it together at different levels at the tree. If the records are in homogeneous structure, could be encrypted by common access structure. This reduces the cost of storing the huge ciphertext as well as time for encrypting each file.

## II. LITERATURE SURVEY

Dynamic. Trait based encryption (ABE) can keep information protection and acknowledge fine-grained get to control. Be that as it may, the thought of document progressive system hasn't been introduced as of not long ago [1]. The issue, the various progressive documents to be shared just utilizing once encryption conspire, can't be adequately explained. In view of the get to structure layered model, a novel get to control plot about record chain of importance is proposed by utilizing ABE to take care of the issue. The proposed plan won't as it were diminish the quantity of get to structures to one, additionally just require a mystery key to decode all the approval records. It is turned out to be secure against the picked plaintext assault (CPA) under the choice bilinear Diffie-Hellman (DBDH) suspicion. Likewise, the execution examination comes about show that the proposed plan is productive and pragmatic when an expansive number of various leveled documents are shared.

Intermediary Re-Encryption (PRE) is a valuable cryptographic primitive that permits a information proprietor to designate the get to privileges of the encoded information put away on a distributed storage framework to others without releasing the data of the information to the genuine however inquisitive cloud server [2]. It gives adequacy to information sharing as the information proprietor notwithstanding utilizing restricted asset gadgets (e.g. cell phones) can offload the greater part of the computational operations to the cloud. Since its presentation numerous variations of PRE have been proposed. A Ciphertext-Policy Property Based Proxy Re-Encryption (CP-ABPRE), which is viewed as a general thought for PRE, utilizes the PRE innovation in the property based encryption cryptographic setting with the end goal that the intermediary is permitted to change over an encryption under a get to strategy to another encryption under another get to approach. CP-ABPRE is material to many system applications, for example, organize information sharing. The current CP-ABPRE frameworks, in any case, leave how to accomplish versatile CCA security as a fascinating open issue. This paper, for the first time, proposes another CP-ABPRE to handle the issue by incorporating the double framework encryption innovation with particular evidence system. In spite of the fact that the new conspire supporting any monotonic get to structures is worked in the composite arrange bilinear gathering, it is demonstrated adaptively CCA secure in the standard model without risking the expressiveness of get to strategy.

Client's security and protection are center issues of system applications [3]. This paper proposes a security insurance model to assess property danger of clients, which considers both affectability of the property and requester's level of affirmation. Besides, the affectability of the property is assessed by issue of expectation-maximization calculation. Tests demonstrate that the ideal size of tests for EM is generally little, which shows the high productivity of the calculation. The proposed security assurance show can't just help clients to do amend approval, additionally advantage the protection reservation of clients in online administration.

In this paper, we propose another thought called k-times characteristic based unknown get to control, which is especially intended for supporting distributed computing condition. In this new idea, a client can confirm himself/herself to the cloud registering server secretly. The server just knows the client gets some required properties, yet it doesn't know the character of this client. Moreover, we give a k-times constrain for mysterious get to control. That is, the server may constrain a specific arrangement of clients (i.e., those clients with a similar arrangement of property) to get to the framework for a most extreme k-times inside a period or an occasion. Encourage extra get to will be denied.

Property based encryption (ABE) frameworks permit scrambling to indeterminate recipients by methods for a get to strategy indicating the characteristics that the proposed collectors ought to have [5]. ABE guarantees to convey fine-grained get to control of scrambled information. Nonetheless, when information are scrambled utilizing an ABE conspire, key administration is troublesome if there is a vast number of clients from different foundations. In this paper, we expound on ABE and propose another flexible cryptosystem alluded to as ciphertext-approach progressive ABE (CP-HABE). In a CP-HABE conspire, the properties are sorted out in a grid and the clients having higher level traits can appoint their get to rights to the clients at a lower level. These components empower a CP-HABE framework to have countless from various associations by appointing keys, e.g., empowering effective information sharing among progressively sorted out expansive gatherings.

Lightweight gadgets, for example, radio recurrence identification labels, have a constrained stockpiling limit [6], which has turned into a bottleneck for some applications, particularly for security applications. Ciphertext-strategy trait based encryption (CP-ABE) is a promising cryptographic device, where the encryptor can choose the get to structure that will be utilized to ensure the touchy information. Nonetheless, current CP-ABE plans experience the ill effects of the issue of having long unscrambling keys, in which the size is straight to also, subject to the quantity of characteristics. This downside keeps the utilization of lightweight gadgets practically speaking as a capacity of the unscrambling keys of the CP-ABE for clients.



In this paper, we give a positive response to the above long standing issue, which will make the CP-ABE exceptionally useful. In this paper, interestingly, we characterize a general thought for intermediary re-encryption (PRE), which we call deterministic limited automata-based useful PRE (DFA-based FPPE) [7]. Then, we propose the first and cement DFA-based FPPE framework, which adjusts to our new thought. In our plan, a message is encoded in a ciphertext related with a discretionary length file string, and a decryptor is honest to goodness if and just if a DFA related with his/her mystery key acknowledges the string. Besides, the above encryption is permitted to be changed to another ciphertext related with another string by a semi trusted intermediary to whom a re-encryption key is given. All things considered, the intermediary can't access the fundamental plaintext. This new primitive can expand the adaptability of clients to assign their decoding rights to others.

Distributed storage and synchronization administrations let clients get to their advanced substance at whatever time, from anyplace, and with any gadget—cell phone, tablet, or desktop PC. It has turned out to be regular for individuals to outsource their information to the cloud without being worried about how the capacity is overseen. In the meantime, the quick appropriation of convenient gear and the developing joining of calculation into purchaser items have brought versatile furthermore, inescapable registering into the standard, with cloud capacity and synchronization benefits generally utilized over cell phones [8]. Many cloud specialist co-ops (CSPs) offer a vast measure of space for buyer utilize. Here we concentrate on Dropbox ([www.dropbox.com](http://www.dropbox.com)), Google Drive ([drive.google.com](http://drive.google.com)), and Microsoft SkyDrive ([skydrive.live.com](http://skydrive.live.com)). Ordinarily, a client who agrees to accept a distributed storage administration can get a couple of gigabytes for nothing or a hundred gigabytes for only a few dollars every month. Clients can get to their information by means of different interfaces, for example, a standard programming customer, a Web program, or a cell phone application. To guarantee the security of a distributed storage benefit, all correspondences amongst clients and the CSP are scrambled, so no one can spy on the information amid transferring or downloading (see the "Related Work in Cloud Security" sidebar). Be that as it may, once clients hand over their information to the CSP and start sharing it with others, the security of that information can move outside their ability to control. Here, we recognize a few security shortcomings in Dropbox, Google Drive, and Microsoft SkyDrive that could lead to information spillage without clients' mindfulness. Moreover, a portion of the shortcomings may exist in other distributed storage administrations, because of the similitude in information sharing techniques.

With the current reception and dissemination of the information sharing worldview in circulated frameworks, for example, online interpersonal organizations or distributed computing, there have been expanding requests and worries for disseminated information security [9]. A standout amongst the most difficult issues in information sharing frameworks is the implementation of get to arrangements and the support of strategies updates. Ciphertext strategy characteristic based encryption (CP-ABE) is turning into a promising cryptographic answer for this issue. It empowers information proprietors to characterize their own get to strategies over client characteristics and uphold the approaches on the information to be circulated. In any case, the preferred standpoint accompanies a noteworthy disadvantage which is known as a key escrow issue. The key era focus could unscramble any messages routed to particular clients by creating their private keys. This is not appropriate for information sharing situations where the information proprietor might want to make their private information just available to assigned clients. Moreover, applying CP-ABE in the information sharing framework presents another challenge with respect to the client renouncement since the get to arrangements are characterized just over the quality universe. Along these lines, in this consider, we propose a novel CP-ABE conspire for an information sharing framework by abusing the normal for the framework engineering. The proposed plot includes the accompanying accomplishments: 1) the key escrow issue could be settled by without escrow key issuing convention, which is built utilizing the safe two-party calculation between the key era focus and the information putting away focus, also, 2) fine-grained client repudiation per each trait should be possible as a substitute encryption which exploits the particular characteristic gathering key dispersion on top of the ABE. The execution and security examinations show that the proposed plan is productive to safely deal with the information conveyed in the information sharing framework.

Cloud registering has risen as a standout amongst the most powerful standards in the IT business lately. Since this new registering innovation obliges clients to depend their profitable information to cloud suppliers, there have been expanding security and protection worries on outsourced information. A few plans utilizing property based encryption (ABE) have been proposed for get to control of outsourced information in distributed computing; be that as it may, the greater part of them experience the ill effects of firmness in actualizing complex get to control arrangements. So as to acknowledge adaptable, adaptable, and fine-grained get to control of outsourced information in distributed computing, in this paper, we propose various leveled characteristic set-based encryption (HASBE) by augmenting ciphertext-approach characteristic set-based encryption (ASBE) with a various leveled structure of clients [10]. The proposed conspire not just accomplishes adaptability because of its various leveled structure, yet, additionally acquires adaptability and fine-grained get to control in supporting compound traits of ASBE. Moreover, HASBE utilizes various esteem assignments for get to close time to manage client renouncement more productively than existing plans. We formally demonstrate the security of HASBE in view of security of the ciphertext-strategy property based encryption (CP-ABE) conspire by Bethencourt et al. what's more, dissect its execution and computational intricacy.

It has been as of late found that a few cyclic gatherings that could be utilized as a part of Cryptography concede an extraordinary bilinear blending map that presents additional structure to the gathering. Bilinear matching maps were first used to break cryptosystems and later it was understood that the additional structure could be misused to construct cryptosystems with additional properties. Boneh and Franklins [11] personality based encryption plot is the most well-known early case of what could be accomplished utilizing bilinear maps. From that point forward, a plenty of cryptosystems have been composed utilizing bilinear maps. No full and unreservedly accessible usage of blending based cryptography was accessible until this work. Later proposition miss the mark concerning this objective as either their source code is not accessible or in light of the fact that they bolster a constrained scope of elliptic bend. In addition, neither one of executes preprocessing that is vital to lessen the calculation time.

In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a client mystery key is related with an arrangement of qualities, and the ciphertext is related with a get to arrangement over qualities. The client can unscramble the ciphertext if and just if the property set of his mystery key fulfills the get to strategy indicated in the ciphertext [12]. A few CP-ABE plans have been proposed, be that as it may, some reasonable issues, for example, characteristic denial, still should be tended to. In this paper, we propose an interceded Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which amplifies CP-ABE with quick quality disavowal.

An Attribute-Based Encryption (ABE) is an encryption plan, where clients with a few characteristics can decode ciphertexts related with these properties. The length of the ciphertext relies on upon the quantity of qualities in past ABE plans [13]. In this paper, we propose another Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with steady ciphertext length. In our plan, the quantity of matching calculations is likewise consistent. What's more, the numbers of extra bits required from picked plaintext assault secure CP-ABE to picked ciphertext assault secure CP-ABE is decreased by 90% as for that of the past plan.

In ciphertext approach property based encryption (CP-ABE), each mystery key is related with an arrangement of traits, and each ciphertext is related with a get to structure on characteristics. Decoding is empowered if and just if the client's characteristic set fulfills the ciphertext get to structure. This gives fine-grained get to control on shared information in numerous pragmatic settings, e.g., secure database and IP multicast. In this paper, we ponder CP-ABE plots in which get to structures are AND entryways on positive and negative qualities. Our fundamental plan is ended up being picked plaintext (CPA) secure under the decisional bilinear Diffie-Hellman (DBDH) suspicion. We then apply the Canetti-HaleviKatz procedure to acquire a picked ciphertext (CCA) secure augmentation utilizing one-time marks. The security confirmation is a lessening to the DBDH suspicion and the solid existential unforgeability of the mark primitive.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) permits to scramble information under an get to strategy, determined as a sensible blend of traits. Such ciphertexts can be decoded by anybody with an arrangement of characteristics that fulfill the get to strategy. We propose a Ciphertext-Policy Attribute-Based Encryption, which depends on a current mystery sharing technique called Linear Integer Secret Sharing Scheme (LISS). In this plan, the encryptor can indicate the get to approach as far as LISS framework  $M$ , over the traits in the framework. The plan is specifically secure under Decisional Bilinear Diffie-Hellman (DBDH) presumption.

### III. SYSTEM ARCHITECTURE

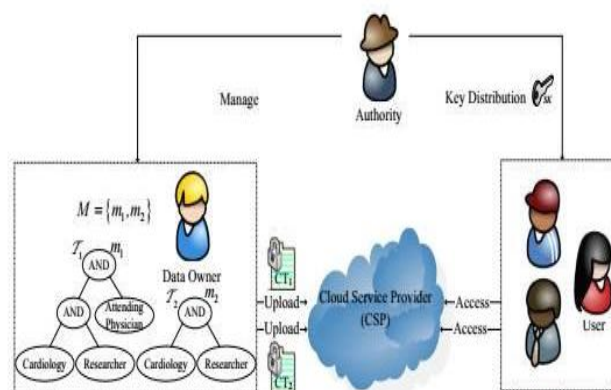


Fig. 1. System Architecture

The architecture of the system consists of Authority, Users, CSP, and the Owner. The authority center accepts the request from user and assigns the relative keys. The authority center is responsible for all key creation and distribution and keeping a record of the owners. The CSP stores the data and provide services. The data owner encrypts the file prior to the sharing and dumping to the cloud. User with the specific key can download the desired record.

IV. METHODOLOGY

In proposed cloud computing scheme, the authority center accepts the request from user and assign the relative keys. The authority center is responsible for all key creation and distribution. The CSP stores the data and provide services. The data owner encrypts the file prior to the sharing and dumping to the cloud. User with the specific key can download the desired record.

The methodology of the current system can be best explained by means of an example. Let us consider the example of a medical center where each of the patient record maintained. To securely share the record the information is divided into sensitive say  $m_1$  and casual medical data  $r_2$ . The laboratory technician for example would require only the  $m_2$  file whereas the physician may be concern with both  $m_1$  and  $m_2$  file. Hence the records are divided as per the variety of access control and the one who want to access the file must be authorized for particular category of files. The picture below describe one such scenario where some researcher can download the medical detail file like Cardiology only, and another user , here attending physician can be able to download the same. The tree for  $m_2$  is submerged in  $m_1$ , therefore we can create a single access tree as shown which reduces the time cost and storage cast.

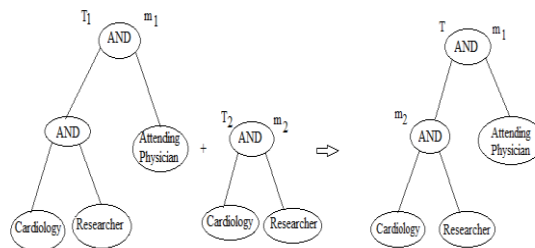
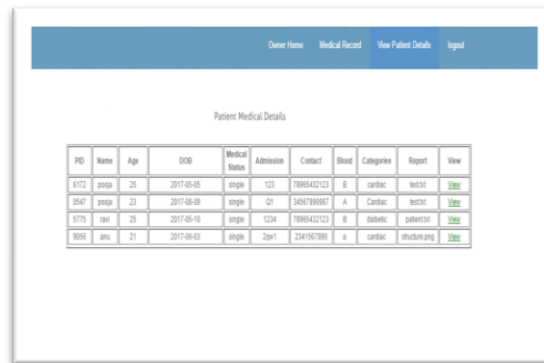


Fig. 2. Cohesive Access Form structure

A. Results

Result is detailed below with figures,



PD	Name	Age	DOB	Medical Status	Admission	Contact	Blood	Categories	Report	View
8172	jeepa	25	2017-05-05	single	123	7895432123	B	cardiac	vector	<a href="#">View</a>
8547	jeepa	23	2017-08-08	single	51	54517891087	A	Cardiac	vector	<a href="#">View</a>
5175	jeepa	25	2017-05-10	single	1234	7895432123	B	diabetic	patient	<a href="#">View</a>
8056	jeepa	21	2017-05-03	single	2001	234567890	a	cardiac	structure.png	<a href="#">View</a>

Fig. 3. It is the file records onto the cloud where the files are all encrypted during upload itself and whenever user requests for file the decryption of file is done using secret key.

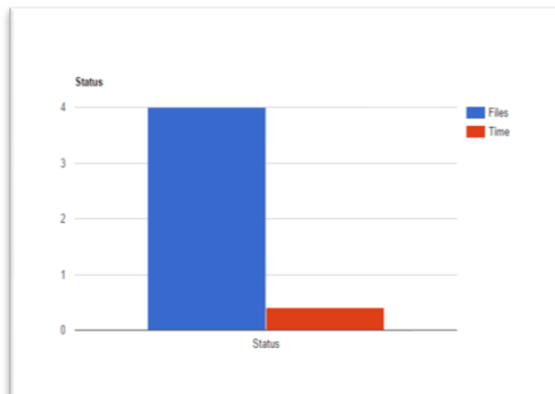


Fig. 4. Graphical representation of file records representing the files sharing with respect to time. Also we see maximum files are shared with minimum consumption of time.



## V. CONCLUSIONS

The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files.

## ACKNOWLEDGMENT

We are thankful towards organization and professors for their positive immense support for us.

## REFERENCES

1. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th Eur. Symp. Res. Comput. Secure., vol. 8712, Sep. 2014, pp. 257–272.
2. K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.
3. T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "k-times attribute-based anonymous access control for cloud computing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep. 2015.
4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13<sup>th</sup> ACM Conf. Comput. Commun. Secur., Oct. 2006, pp. 89–98.
5. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.
6. X. Xie, H. Ma, J. Li, and X. Chen, "An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing," J. Universal Comput. Sci., vol. 19, no. 16, pp. 2349–2367, Oct. 2013.
7. Balu and K. Kuppusamy, "An expressive and provably secure ciphertext-policy attribute-based encryption," Inf. Sci., vol. 276, pp. 354–362, Aug. 2014.
8. J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," Future Generat. Comput. Syst., vol. 52, pp. 67–76, Nov. 2015.
9. K. Liang et al., "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," Future Generat. Comput. Syst., vol. 52, pp. 95–108, Nov. 2015.
10. Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.
11. H. Deng et al., "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," Inf. Sci., vol. 275, pp. 370–384, Aug. 2014.
12. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proc. 35th Int. Colloq. Automata, Lang. Program., vol. 5126, Jul. 2008, pp. 579–591.
13. J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.
14. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Conf. Secur., Aug. 2011, pp. 1–16.