© 2018 IJSRSET | Volume 4 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

An Attribute-Based Encryption Scheme in Cloud Computing for Efficient File Hierarchy

Priyanka Thevarkar, Anuja Pendpalle, Ankita Bonde, Prof. Ashish Sonawane
NBN Sinhgad School of Engineering, Pune, Maharashtra, India

ABSTRACT

Ciphertext-policy characteristic-primarily based encryption (CP-ABE) has been a favoured encryption generation to solve the tough hassle of comfy records sharing in cloud computing. The shared records documents generally have the feature of multilevel hierarchy, especially within the location of healthcare and the military. But, the hierarchy structure of shared files has not been explored in CP-ABE. In this paper, an green file hierarchy characteristic-primarily based encryption scheme is proposed in cloud computing. The layered get entry to systems are incorporated into an unmarried get right of entry to structure, and then, the hierarchical files are encrypted with the included get admission to shape. The ciphertext additives associated with attributes may be shared by means of the files. Consequently, each ciphertext garage and time price of encryption are saved. Moreover, the proposed scheme is proved to be relaxed underneath the usual assumption. Experimental simulation shows that the proposed scheme is highly green in phrases of encryption and decryption. With the quantity of the documents increasing, the blessings of our scheme grow to be increasingly more conspicuous.

Keywords: Ciphertext, CP-ABE, CSP

I. INTRODUCTION

With the burgeoning of network generation and mobile terminal, on line records sharing has grow to be a new “pet”, together with facebook, MySpace, and Badoo. in the meantime, cloud computing is one of the most promising application systems to resolve the explosive increasing of information sharing. In cloud computing, to defend facts from leaking, customers need to encrypt their information earlier than being shared. Get right of entry to control is paramount as it's far the first line of protection that forestalls unauthorized get admission to the shared records. These days, characteristic-primarily based encryption (ABE) has been attracted an awful lot greater attentions given that it can keep facts privateness and realizes nice-grained, one-to-many, and non interactive get entry to manipulate. Ciphertext-coverage attribute based totally encryption (CP-ABE) is one in every of viable schemes which has much greater flexibility and is greater appropriate for well known packages.

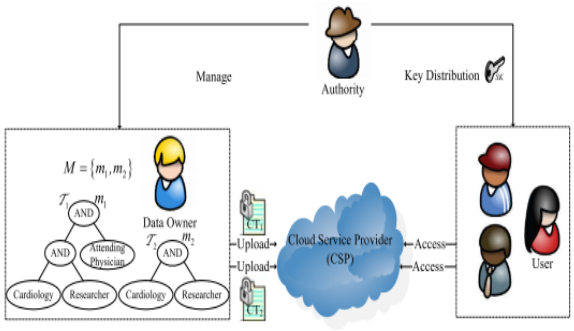

Figure 1. An Example of Secure Data Sharing In Cloud Computing.

T1 and T2 access structures of m1 and m2, respectively .T is the included get entry to structure of m1 and m2. In cloud computing, as illustrated in Figure 1, authority accepts the consumer enrolment and creates some parameters. Cloud provider (CSP) is the manager of cloud servers and provides more than one services for client. Data proprietor encrypts and uploads the generated ciphertext to CSP. Person download sand decrypts the fascinated ciphertext from CSP. The shared documents usually have hierarchical structure. That is, a

collection of documents are divided into some of hierarchy subgroups placed at distinct get entry to levels.

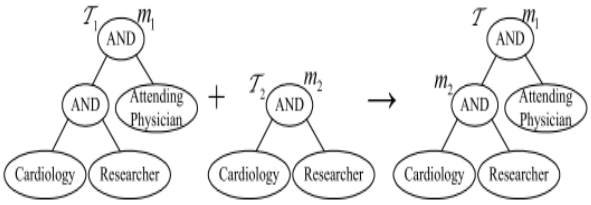

Figure 2. The Integrated Access Structure

If the documents within the equal hierarchical structure may be encrypted by using an included get right of entry to shape, the storage value of ciphertext and time fee of encryption can be saved. Here let us take the non-public fitness record (PHR) for example. To safely percentage the PHR records in cloud computing, a affected person divides his PHR records Minto two parts: personal statistics m1 that could contain the patient's name, social safety range, telephone quantity, home cope with, etc. The clinical file m2 which does not contain sensitive personal statistics, along with medical test consequences, remedy protocols, and operation notes. Then the patient adopts CP-ABE scheme to encrypt the informationm1 and m2 by way of extraordinary access rules primarily based at the actual need. for instance, an attending medical doctor needs to access both the affected person's name and his medical document in order to make a diagnosis, and medical researcher only desires to access some medical check outcomes for academic reason in the related vicinity, wherein a medical doctor need to be a scientific researcher, and the communicate is not always real. Suppose that the patient sets the get entry to shape of m1 as: T1 ("Cardiology "AND "Researcher") AND "Attending physician". Further, m2 is termed as: T2 "Cardiology" AND "Researcher". The example is deployed in cloud system as shown in Fig. 1.seemingly, the records needs to be encrypted twice ifm1 and m2 are encrypted with access structures T1 and T2,respectively. Two ciphertext CT1 = T1, C ˜1, C1, ∀y ∈Y1: Cy, Cy wherein Y1="Cardiology", "Researcher", "Attending Physician" and CT2 = T2, C ˜2, C2, ∀y ∈ Y2: Cy, Cy whereY2="Cardiology", "Researcher" can be produced [11]. Within the Fig. 1, we can find that the two get right of entry to systems have hierarchical relationships wherein the access shape T1 is the extension of T2. The 2 structures can be included into one structure T as shown in Fig. 2. If the two documents will be encrypted with the included get right of entry to shape and produce ciphertext CT = T, C ˜, C, ∀y ∈ Y: CY, Cy where Y="Cardiology", "Researcher", "Attending medical doctor". Right here, the additives of ciphertext T , Cy, Cy are related to coverage. Mean while, access structure could be shared by the two documents. Therefore, the computation complexity of encryption and storage overhead of ciphertext may be reduced substantially.

Moreover, since delivery nodes (talk to Figure 3below) are brought inside the get admission to structure, customers can decrypt all authorization documents with computation of secret key once. The computation cost of decryption can also be reduced if users want to decrypt a couple of files on the same time. Display that FH-CP-ABE has low garage fee and computation complexity in phrases of encryption and decryption. It has to be observed that the proposed scheme differs from the subsequent CP-ABE schemes, which utilize the consumer layered version to distribute the work of key creation on a couple of area authorizations and lighten the load of key authority middle. Similarly, the part of these paintings is offered in. The work supplied in that conference paper is rough and incomplete, where some critical aspects haven't been considered.

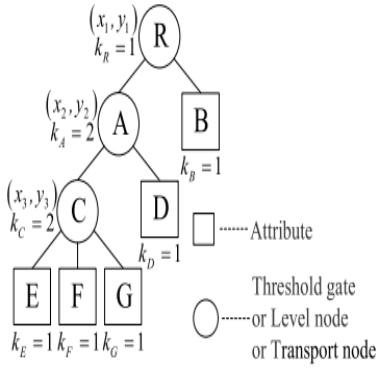

Figure 3. An example of three-level access tree.

II. EXISTING SYSTEM

Sahai and Waters proposed fuzzy identification-based totally Encryption (IBE) in 2005, which turned into the prototype of ABE. Latterly, a variation of ABE named CP-ABE changed into proposed. due to the fact that Gentry and Silverberg proposed the primary perception of hierarchical encryption scheme, many hierarchical CP-ABE schemes were proposed. for example, Wang et

al. proposed a hierarchical ABE scheme by means of combining the hierarchical IBE and CP-ABE.

Wan et al. proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, at the same time as the duration of secret key's linear with the order of the attribute set. A ciphertext policy hierarchical ABE scheme with quick ciphertext is also studied. In those schemes, the figure authorization area governs its child authorization domain names and a pinnacle-stage authorization domain creates mystery key of the following-degree area. The paintings of key advent is sent on more than one authorization domains and the weight of key authority centre is lightened.

III. SURVEY WORK

1. Ciphertext-policy Hierarchical attribute-primarily based Encryption for exceptional-Grained access control of Encryption facts : within the ciphertext-coverage attribute based encryption (CPABE) scheme, a private key holder is related with a set of attributes even as the data is encrypted below an get right of entry to shape defined via the records company. In most proposed schemes, the traits of the attributes are dealt with as identical level. Even as within the actual world condition, the attributes are constantly within the specific stages. on this paper, in this paper, a scheme is proposed underneath a specific hierarchy of attributes with the name of ciphertext-coverage hierarchical attribute based encryption. The CP-HABE scheme is proved to be secure underneath the decisional q-parallel bilinear Diffie-Hellman exponent assumption, which may be considered as the generalization of the traditional CP-ABE. in this paper, we advocate a scheme referred to as ciphertext coverage hierarchical attribute based encryption in which the attributes inside the device aren't constantly in the same level. We gift unique production of CP-HABE which uses the hierarchical get admission to shape that can be considered as a generalization of conventional ABE.

Best while a hard and fast of attributes possessed by using the consumer satisfies the hierarchical access structure can he/she decrypt the ciphertext. We additionally provide a safety version for CP-HABE. Eventually, we show our scheme underneath the security model by reducing it to decisional q-parallel bilinear Diffie-Hellman exponent assumption. more importantly, this construction can show off substantial development over the traditional ABE schemes accordant with the practical state of affairs.

2. Extended Proxy-Assisted approach: attaining revocable first-rate-Grained Encryption of Cloud information: attribute-based encryption has the potential to be deployed in a cloud computing surroundings to offer scalable and fine-grained facts sharing. However, person revocation within ABE deployment stays a hard trouble to triumph over, specifically when there may be a big number of customers. in this work, we introduce an extended proxy-assisted approach, which weakens the agree with required of the cloud server. Primarily based on an all-or-nothing principle, our method is designed to deter a cloud server from colluding with a 3rd birthday celebration to avert the user revocation functionality. We demonstrate the application of our technique through providing a creation of the proposed approach, designed to offer green cloud data sharing and consumer revocation. A prototype turned into then applied to illustrate the practicality of our proposed production. On this paper, we supplied an prolonged proxy-assisted approach in order to triumph over the quandary of desiring to agree with the cloud server not to disclose customers' proxy keys inherent in proxy/mediator assisted person revocation methods. In our approach, we bind the cloud server's non-public key to the records decryption operation, which requires the cloud server to reveal its personal key should the cloud server determine to collude with revoked users. We then formulated a primitive, 'revocable cloud records encryption', underneath the method. We provided a concrete construction of the primitive and carried out the development the usage of a proof-of-idea. The experimental effects cautioned that our construction is appropriate for deployment even on clever mobile devices.

3. Cozy sharing of personal fitness information in cloud computing: Ciphertext-policy attribute-based encryption: Online non-public fitness file (PHR) enables patients to manipulate their very own scientific facts in a centralized way, which significantly facilitates the garage, get entry to and sharing of personal health statistics. With the emergence of cloud computing, it is attractive for the PHR service carriers to shift their PHR packages and garage into the cloud, on the way to experience the elastic assets and reduce the operational price. But, by way of storing PHRs in the cloud, the sufferers lose physical control to their private health

data, which makes it important for every patient to encrypt her PHR information before importing to the cloud servers. Below encryption, it's far difficult to attain fine-grained get entry to manage to PHR statistics in a scalable and efficient way. For every affected person, the PHR statistics need to be encrypted so that it's miles scalable with the variety of customers having get entry to. also, for the reason that there are multiple proprietors (patients) in a PHR gadget and every owner would encrypt her PHR documents the use of a exceptional set of cryptographic keys, it's far crucial to lessen the important thing distribution complexity in such multi-owner settings. Existing cryptographic enforced get entry to manipulate schemes is typically designed for the unmarried-proprietor eventualities. On this paper, we advocate a unique framework for get admission to manage to PHRs within cloud computing surroundings. To enable first-rate-grained and scalable get right of entry to manage for PHRs, we leverage attribute primarily based encryption (ABE) techniques to encrypt every sufferers' PHR information. To reduce the important thing distribution complexity, we divide the device into a couple of protection domain names, wherein every domain manages most effective a subset of the users. in this way, every patient has full control over her own privateness, and the key control complexity is decreased dramatically. Our proposed scheme is likewise flexible; in that it supports green and on-demand revocation of user get right of entry to rights, and break-glass get entry to under emergency situations.

IV. OVERVIEW OF SYSTEM

Hassle declaration

The problem declaration system best requires a semi-depended on third birthday celebration, chargeable for carrying out easy matching operations successfully.

Evaluation

Ciphertext-policy characteristic-based encryption (CP-ABE) has been a desired encryption technique to solve the difficulty of relaxed records sharing in cloud computing. The shared data documents normally have the houses of multilevel hierarchy, especially in the location of healthcare and the navy. However, the hierarchy shape of shared documents has no longer been explored in CP-ABE. in this paper, an powerful document hierarchy attribute-primarily based encryption technique is proposed in cloud computing. The layered access systems are blanketed right into a single access structure, and then, the hierarchical files may be encrypted with the integrated get admission to shape. The cipher textual content additives just like attributes could be shared by the files. Consequently, each ciphertext storage and time value of encryption are maintained. Moreover, the proposed scheme is proved to be relaxed under the prevalent assumption .Experimental simulation shows that the proposed approach is extra effective in terms of encryption and decryption. With the range of the files growing, the benefits of our approach turn out to be more and cleaner.

V. ADVANTAGES OF PROPOSED SYSTEM

1. To manipulate scheme for comfortable information garage in clouds that helps nameless authentication.
2. Inside the proposed scheme, the cloud verifies the authenticity of the series without knowing the consumer's identity earlier than storing records.
3. Our scheme additionally has the delivered characteristic of access control wherein most effective valid customers are able to decrypt the saved records.
4. The scheme prevents replay assaults and helps advent, change, and analyzing statistics saved within the cloud.
   - ✓ Allotted get admission to control of records stored in cloud in order that best authorized users with legitimate attributes can access them.
   - ✓ Authentication of users who shop and alter their information at the cloud.
   - ✓ The identification of the user is covered from the cloud throughout authentication.
   - ✓ The existing scheme is likewise relaxed in opposition to user collusion assaults due to use of attribute-primarily based encryption.
   - ✓ The experiments display that the prevailing scheme is applicable on Smartphone, in particular whilst a cloud platform is available.
   - ✓ To offer an get admission to manipulate scheme for scalable media. The scheme has several blessings which make it particularly appropriate for content shipping.

VI. CONCLUSION

To proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing. 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. Moreover, the proposed scheme is proved to be secure under DBDH assumption.

VII. REFERENCES

[1]. C.-K. Chu, W.-T.Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50-57, Oct./Dec. 2013.

[2]. T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int.Conf. Inf. Secur. Pract.Exper., vol. 8434. May 2014, pp. 346-358.

[3]. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014,pp.257-272.

[4]. T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014, pp. 130-147.

[5]. 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.

[6]. 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.

[7]. J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for Web-based cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484-497, Mar. 2016.

[8]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp. 457-473.

[9]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun.Secur., Oct. 2006, pp. 89-98.

[10]. W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," Chin. J. Electron., vol. 23, no. 4, pp. 778-782, Oct. 2014.