WWJMRD 2018; 4(1): 11-15
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Sajja Pavan
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Gopichand G
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Santhi H
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Gayathri P
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Correspondence:
Sajja Pavan
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Secured Privilege Separation on Cloud Services

Sajja Pavan, Gopichand G, Santhi H, Gayathri P

Abstract
The swift development of computer technology and the cloud based services are currently the hot topics. They give clients comfort and bring many security issues as well, let's say information sharing and the security issue. In this project we are going to present a control framework with privilege separation in view of security assurance which deals with two types of users mainly called public and private consistently. In private user for achieving the write access and read access we are adopting Attribute based signature and Aggregate encryption respectively. In public user we are going to establish an Attribute encryption method with the efficient decryption in order to eliminate the issue like distributing the complicated key.

Keywords: Attribute based signature, Aggregate encryption, Attribute encryption Complicated key

Introduction
Rapid improvement in the domain of cloud computing, cloud services is widely used. The individual can hide his information in cloud. Here the major concern is cloud security. It is mandatory to ensure the privacy of the data. In order to improve the security this system is developed. We observed that with the existing models are not much effective in doing this while sharing the data. These data sharing issues has put a stop for the development of the cloud computing. So many people have implemented various solutions for achieving encryption and the decryptions of the data sharing are proposed. In 2007 bethencourt first proposed ciphertext attribute based encryption. In this revocation is not considered. In 2011 Hur put forward the fine revocation process and again usage of this one cause's key issue. And lewko used the multi authority to solve the key issues. And again the accessibility is not that much flexible for this case. Li has given the solution in the form of method which helped for the data sharing on systematic encryption which gives the different users the different accessibility rights. But this also does not make any difference from complexity and efficiency. In 2014 Chen came up with aggregate encryption which effectively shortens the length of ciphertext and key. But this is useful only when the data owner knows the identity of the particular person. The above mentioned cases do not have the standards. In this paper we present a separation based method and the following points are like protocols.

a. We are proposing a new access system which is privilege separation based one. Here the system uses the aggregate encryption algorithm and Hierarchy attribute based encryption algorithm to perform the read access in private and public user respectively. The key encryption algorithm effectively improves accessibility purposes and hierarchy attribute encryption gives privacy to the user data.
b. Now the system is compared with Multi authority Hierarchy attribute encryption which does not give any write permissions to private user and we are using improved attribute based encryption. For this purpose. By this the user can cloud server signature verification without any identity and the user can modify file with ease.
c. Hence we are providing the brief analysis of complex and security reasons of above method.

Literature survey:
This paper goes for fine-grained data get the chance to control conveyed processing.

One test in this setting is to finish fine grainedness, data order, and flexibility. In the meantime, this isn't given by current work. In this paper we propose an arrangement to fulfill this goal by KP-ABE and especially going along with it with systems of middle person re-encryption and drowsy re-encryption. Also, our proposed plan can enable the data proprietor to dole out the lion's share of figuring overhead to viable cloud servers.

Order of the customer get to the advantage and customer riddle for key obligation can be expert. Formal security proofs exhibit that our proposed plot is secure under standard cryptographic models. Later, we performed inquiries in the picked databases. Since the watchword "Disseminated processing" passed on too much various results for a separated affirmation, we added more catchphrases to our request. These watchwords were security, protection, security course, data security, and data affirmation. In addition, Cloud Computing contracts are generally considered as data taking care requests contract law[1].

In this we incredibly diminish the multifaceted nature of key administration alongside the security looked at. Utilizing ABE to encode the information, so clients can enable access to various spaces/territories with the various expert parts, capabilities. We upgrade the current ABE plan to deal with the productive and request client repudiation, and demonstrate security[2].

Despite the fact that the quantity of Cloud Computing clients is consistently expanding, a few factors still keep a more fast dispersal of the technique, for instance, specialized criteria as adaptability or particularly law issues like the information assurance and the privacy[3]

In Hansen's (2012) feeling, another issue is the examination of data by the client. Besides that, too much couple of information manufactures the nonattendance of straightforwardness. Remembering the true objective to find a predominant change in this issue, the General Data Protection Regulation plans to explicitly address the issues that rise up out of the commitment to exhort and to disclose[4]

All things considered, using Cloud applications induces the limit and treatment of data on external servers. This generally prompts a diminished expert for the remitter[5]

Everything considered, the data get to is directed by the data proprietor. Second, by join get to benefits in metadata record, an endorsed customer can decipher a mixed report just with his private key. These game plan is in like manner gave off an impression of being impenetrable to unapproved access to data and to any data exposure in the midst of sharing technique, given that two levels of access control verification[9].

Cloud computing is getting to be noticeably prominent these days. Organizations like, Microsoft, Amazon, Google, IBM and others are embracing cloud frameworks and moving their administrations to cloud to lessen the cost and draw in more clients [10]. In another work, the creators displayed the access control component in view of the idea of put stock in registering [11]. Their framework reviews and inspects every client that gets to the cloud information and assets.

The framework forces high security and protection, yet the procedure of reviewing and inspecting every client turns out to be progressively mind boggling when the system movement increments.

Meghanathan introduced an audit of existing access control models for distributed computing and separated the current access control models into three unique classifications: (1) part based models, (2) quality based encryption models, and (3) multi-occupancy models. The creator introduces the upsides and downsides of each model.

To get more understanding on every class the peruser is welcome to peruse this survey [12] The access control strategy has been broadly utilized as one of the promising security arrangements with regards to information/asset security and provisioning.

It generally works in view of the access strategies characterized by framework executives.

The access control approaches can be characterized on any layer or segment of the framework. For instance, access to records can be characterized on document servers, access to web benefits on web servers, etc.

These security approaches are characterized from multiple points of view and at various levels. The access control list (ACL for short) is one of the components which helps the framework executive characterize the security and access approaches for their framework. The ACL is a consecutive rundown with permit/deny passages characterized for the administrations and assets that are accessible for true blue clients at any given time. ACLs guarantee that exclusive true blue clients access the approved administrations by Providing movement separating, security strategy execution, client provisioning and so forth [15]

In another work, Almutairi exhibited the Distributed Access Control Architecture for Cloud Computing in view of standards drawn from security administration to meet the client's access control necessities and standards attracted from programming building to produce security prerequisite details. Their answer can be executed utilizing a XML-based formalism which makes it less demanding to actualize in the present administration model of distributed computing [16]

In another exertion Li [14] exhibited an access control strategy for social insurance applications where numerous clients can get to their information in the cloud condition. The creators displayed an adaptable novel access control system in light of the trait based encryption (ABE) strategies that encode every patient's Personal Health Record (PHR) information.

Their framework is separated into different security spaces, where every area oversees just a subset of the clients. This framework division lessens the key circulation multifaceted nature which is an imperative segment in such multi-proprietor settings. Be that as it may, encryption key dispersion among clients remains an open inquiry when managing various sending models and getting to benefit over the cloud conditions

In another exertion, Li [13] displayed a personality based access control strategy to secure the access to the cloud administrations. The creators exhibited a personality based various leveled demonstrate for distributed computing (IBHMCC) and its comparing encryption (i.e. character based encryption (IBE)) and mark (i.e. character based mark (IBS)) conspires and contrasted their outcomes and the conventional SSL Authentication Protocol (SAP). The creator contended that their answer is lightweight and more effective than SAP. The arrangement is most appropriate for private mists. No confirmation about the execution of this framework in the general population cloud and with various security models is given.

Proposed methodology:

This proposed method consists of the following modules like Data owner, people in public user, people in private user, root authority, cloud service provider. The cloud service provider will mainly contain two components one is like for data storage and other is for data service. Storage is mandatory for the storage of the files and the data service is mainly responsible for controlling the external users accessibility for secret data and related ciphertext.

The root authority actually manages the sources in its own place. And now again the attributes that are owned by users are issued by separate authority but not the same. Now the private user which is having the personal list like close friends, family, relatives etc and this domain is having very few members in it and it is easy to manage and also the data owner knows identity of the people in it.

Coming to the public user, generally it contains large number of users in it with the unknown identity and the lot of attributes are owned by the user. Last thing is that the Data owner, he manages to encrypt the uploaded files using the corresponding encryption method and there by sending it to the cloud server and it is totally based on the characteristics of the private and the public users in it in order to control the accessibility.

Private user read and writes accessibility:

In case of reading, as it is having few members their identities are known to the data owner. In this context the data owner wants only the users to modify the data and then the different users can access and modify different parts. Like suppose we have a facebook account and only our friends are able to see the posts followed by us and others may not be due to the security settings arranged by you. And in this case if anyone wants to see the data, he needs the data owner to grant the permission for either read or write for that particular data. Mainly in this private user people will be having the close relationship so we are using aggregate encryption method and eventually it improves access efficiency since it is having

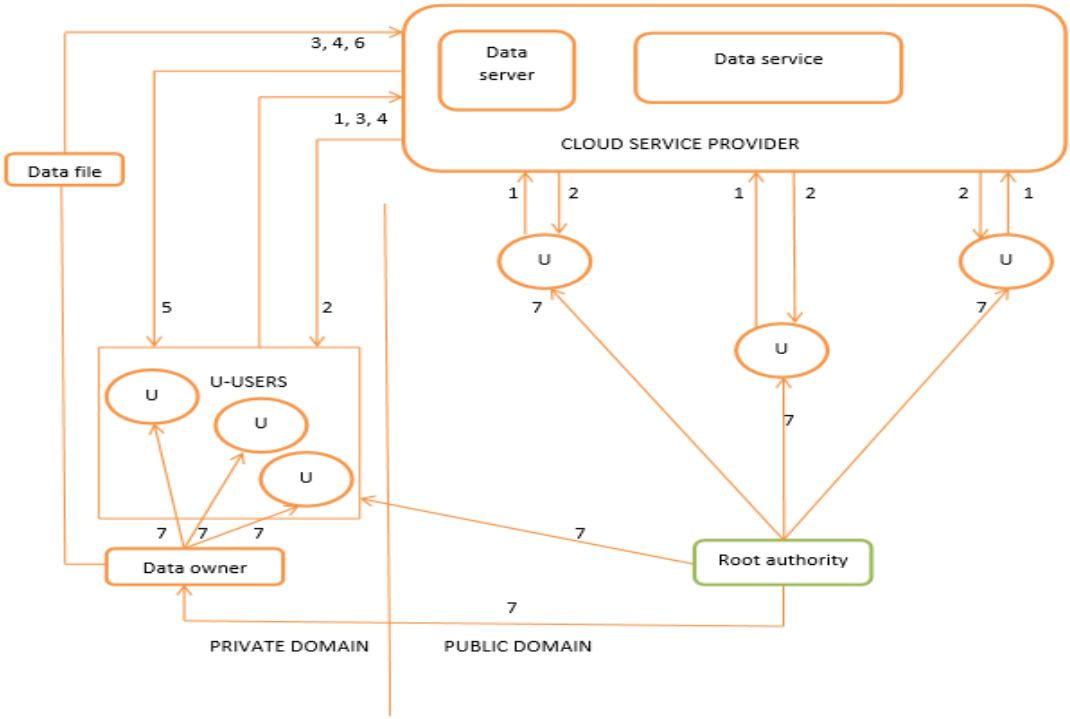

Fig.1: Proposed Framework

Here the following terminology is followed:

1. Requesting a file
2. Returning of the ciphertext
3. Modifying the file
4. Uploading the encrypted file
5. Verification
6. Deleting the files
7. Distribution of keys

Small number of users with the identities knows to data owner. Here we can use Attribute based encryption also but for managing the keys and attributes the process is a bit complex one and this method is mainly applicable for large number of users so that is why we are not adopted this one.

So for reading the data the aggregate key encryption algorithm is as follows.

1. The system is going to run the setup of aggregate encryption for the establishment of the public system and the master key.
2. There will be the classification of the files based on the attributes so one class file cannot be the subset of another class file.
3. Now the owners application runs the encrypt of the aggregate encryption using key and also with the help of classification file number and then encrypts it's and sends that to the cloud.
4. Now when the user puts the request to cloud server with the file number then the cloud server will return the encrypted file to the corresponding user.
5. Then the owner known users will be given permission with the file number and is further processed to root authority.
6. Now the root authority generates the aggregate decryption key for the following file number with the help of extract and will be sent to the corresponding user.

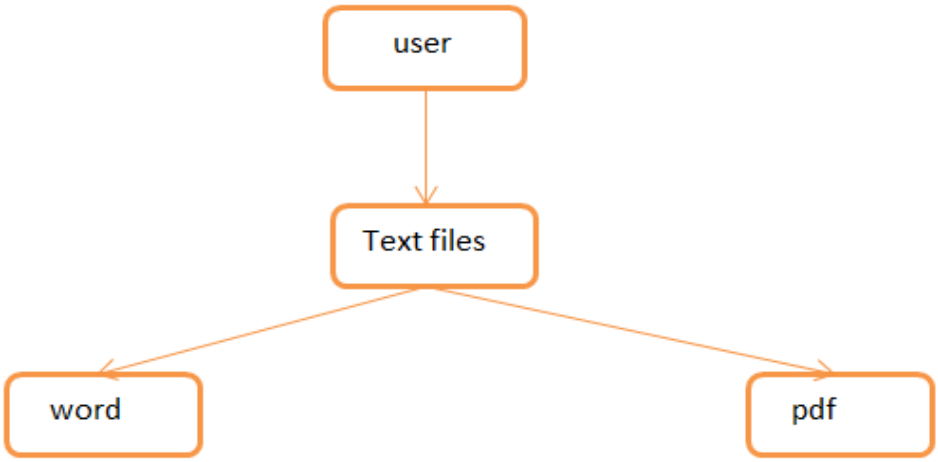

Fig.2: File type classification

In case of writes if someone who is so close to owner needs to modify the files in the cloud he needs permission. After the reading of the file the user can modify since he knows the key and the file number so he can do the implementation of the algorithm to encrypt the files after certain modification and he can upload them to the cloud. But here is the case that cloud server accepts or let's say saves depends on the write control process. In this aspect the separate read and write are extremely important. In private user it is not like that all the users having read access must have the write access. This is mainly decided by the data owner.

So in order to decide that we are using improved attribute based signature for the determination of the users write access. And this structure mainly includes 5 components like data owner, root authority, user, mediator and the cloud servers. The root authority generates the master key and sends it to the data owner and for the system which in turn shared to all the users.

Here the mediator is holding the components of the respective signature and will be helpful for the validity check of the users. Here the data owner makes the signatures and directly it sends to the cloud. Then the user who ever has modified the files and uploaded them into the cloud has to match with the attribute based signature if it is fine then the modified file will be saved to the cloud or else won't.

Public user accessibility:

It is mainly for large number of users having a lot of attributes. Complex in managing those and the indefinite user count all these terms can have only read accessibility. Even though the attribute based encryption can give the access control certainly it is not going to meet the complex cloud. In this the data owner will give the access policies and also encrypts the files according to the policy. Now the each of the user is distributed a key as long as he is following the policy the individual can decrypt file. Let's say if we have only one authority in the framework certain problems will be arise. We can see those in detail. Practically there will be lot of authorities and they can manage their own field of users. Now again the attributes owned by the user are issued by different authorities but not the same authority.

And in case of only one authority all the distributions of keys are being done by the one authority and leading to potential risks. The users in this domain mainly do not need to interact with the data owner here the owner uploads the data files to the cloud server and after authorization he will receive the decryption key and the owner sends the file request for accessibility form the cloud server and then the cloud server returns the ciphertext by now the users can use their decryption keys to decrypt.

The algorithm for the Hierarchy attribute encryption is as follows:

1. The files are being created by the data owner and in order to protect the privacy of the files owner encrypts the file and then sends it to the cloud environment. In order to reduce the complexity involved in it the owner will combine the symmetric and the key encryption methods.
2. Selecting the unique ID for the file and choose the random symmetric encryption key and encrypt it. Before encrypting the files we need to define the access tree using the algorithm and pass the ciphertext.
3. Now the data owner will be computing the ciphertext using hash operations and signs the ciphertext and will get the signature. One purpose served with this is it ensures the data integrity and other is that it will facilitate both the user and cloud to authenticate the identity of the data owner.
4. Whenever the user wants the data file he should get the file from the cloud and decrypt it. It has two process to be done while decrypting the file. First we use the algorithm to decrypt the symmetric key and then with the help of the symmetric key we can decrypt the data file.
5. In case if the data owner wants to delete a particular file form the cloud he should send a file id along with his signature to the cloud now the cloud server deletes the corresponding file after verification.
6. There will be particular time limit to access the data files like authority assigns the attributes to each individual and sets the expiration time. There will be a tree which should match with the attributes so the data can be accessed.
7. And the attributes revocation will be done by setting the new expiration time and generating the new private key components and will be returned to the client.

Conclusion

In this paper we proposed a method which is called privilege separation on privacy issues. We have done analysis of cloud environment and the user characteristics and based on that the users are being divided into two types called public and private users. In private user we used the aggregate encryption algorithm for the users read accessibility and improved attribute based signature for the write accessibility. This gives the separation for reading and writing which in turn protects the user's identity. Whereas in public user we used hierarchy attribute encryption for data sharing.

References

1. V. sathyapreiya "secure role based data access control in cloud computing" international journal of computer trends and technology- may to june issue 2011.
2. Hulawalekalyani" achieve fine grained data access control in cloud computing using kp-abe along-with lazy and proxy re-encryption" international journal of emerging technology and advanced engineering volume 4, issue 2, february 2014).
3. Borges, G.; Brennschneidt, K.: Rechtsfragen des Cloud Computing – ein Zwischenbericht. In Borges, G.; Schwenk J. (Eds.): Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Springer, Berlin, 2012, pp. 43-77.
4. Hansen, M.: Datenschutz im Cloud Computing. In Borges, G.; Schwenk J. (Eds.): Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Springer, Berlin, 2012, pp. 79-95.
5. [5] Matros, R.; Rietze C.; Eymannm T.: SaaS und Unternehmenserfolg: Erfolgskategorien für die Praxis. In Benlian, A. (Ed.): Software-as-a-Service Anbieterstrategien, Kundenbedürfnisse und Wertschöpfungsstrukturen. Gabler, Wiesbaden, 2010, pp. 239-254.
6. M. Nabeel and E. Bertino. "Towards the attribute based group key management," in Proceedings of the 18th ACM conference on Computer and the communications security, Chicago, Illinois, USA, 2011.
7. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the public cloud," in IEEE Transactions on the Knowledge and Data Engineering, 2014
8. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as the service model" in the IEEE International Conference on Information Reuse and the Integration (IRI), 2012.
9. Nesrine Kaaniche, Maryline Laurent," A Secure Client Side Deduplication Method in Cloud Storage Environments" 6th International Conference on new Technologies, Mobility and Security year 2014.
10. Ahmed, M., & Hasibuan, Z. A. (2012). E-Government based on cloud environment in indonesia. Seminar Nasional Aplikasi Teknologi informasi. yagyakarta
11. Shaikh, F. B., & Haider, S. (2011). Security threats in cloud computing. Internet technology and secured transactions (ICITST), 2011 international conference for, (pp. 214-219).
12. Maghanathan, N. (2013). Review of access control models for cloud computing. Computer Science & Information Science, 3(1), 77-85.
13. Li, H., Dai, Y., Tian, L., & Yang, H. (2009). Identity-based authentication for cloud computing. In Cloud computing (pp. 157-166). Springer Berlin Heidelberg.
14. Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multiowner settings. In Security and Privacy in Communication Networks (pp. 89106). Springer Berlin Heidelberg
15. Tsai, W., Jin, Z., & Bai, X. (2009). Internetware computing: issues and perspective. In: Proceedings of the first Asia-Pacific symposium on Internetware., 1–10.
16. Almutairi, Abdulrahman A., et al. "A distributed access control architecture for cloud computing." IEEE software 2 (2011): 36-44.