International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Secure and Error-Free Data Storage on Cloud via Deniable CP-ABE Scheme

Vanitha M, Mangayarkarasi R, Sumaiya Thaseen I, Saira Banu J

Abstract: ***Cloud storage services are quickly increasing and more prevalent. CSP-cloud storage providers offer storage as a service to all the users. It is a paid facility that allows association to outsource their confidential data to be stored on remote servers. But, identity privacy and preserving data from an untrusted cloud is a difficult concern, because of the successive change of the members. CSP has to be secured from an illegitimate person who performs data corruption over cloud servers. Thus, there is a need to safeguard information from the individuals who don't have access by establishing numerous cloud storage encryption plans. Every such plan implemented expects that distributed storage suppliers are protected and can't be hacked; however, practically speaking, a few powers will compel distributed storage suppliers to render client details and secret information on the cloud, in this manner inside and out bypassing stockpiling encryption plans. In this paper, a new scheme is introduced to protect user privacy by a deniable CP_ABE(Cloud Provider_ Attribute Based Encryption) scheme which implements a cloud storage encryption plan. Since coercers cannot specify whether privileged insights are valid or not, the CSP ensures privacy of the user.***

Index Terms: cloud storage, Cloud servers, Encryption

I. INTRODUCTION

Cloud storage services have quickly turned out to be progressively famous. Anywhere at any time users can store and have right to access the data or information on the cloud. As a result of user security, the information put away on the cloud is regularly encoded and shielded from access by different clients. Amongst the most suitable encryption technique is attribute-based encryption (ABE) which is viewed as a standout for Cloud storage, in view of the collaborative property of the cloud information[6] . Many trusted third parties and cloud storage providers handle key management technique for encryption which are reliable and cannot be hacked. Now-a-days, any intruder can stop the communication in between the user and cloud storage providers and even they may force or compel cloud to provide confidential data of user by claiming as if they have original authority. In the above situation, attacker demand storage providers in order to get user secrets and to know the encrypted data.

Manuscript published on 30 August 2019.
*Correspondence Author(s)
V**anitha M,** Associate professor in VIT, Vellore.
Mangayarkarasi Ramaiah, Associate professor in the School of Information Technology and Engineering at VIT University, Vellore, India.
Dr. Sumaiya Thaseen, has thirteen years of teaching and research experience in VIT University.
J. Saira Banu, is working as a faculty at School of Computing Science and Engineering, VIT University, Vellore.

Agreement terminates when we move the files starting with one cloud then onto the next cloud nature's domain, the customer can request to deny the file policy. The Policy will be revoked and the key director will entirely clear the public key of the associated file at the point when any of the above criteria exist. In future no one can retrieve back the control key of a revoked file. Therefore we can say the record is absolutely deleted. The Key supervisor produce public key under the request by the user to recover the file. For that the client must be checked. To access the file we use key policy attribute based encryption standard. It is verified with an attribute connected with the file. The file arrangement may be read just or write underpinned when downloaded from the cloud with the file access control. Each customer has associated with methodologies for every one record. So the right customer will get to the right record.

Considering the cloud storage service, many deniable key schemes are bitwise in which the scheme can only use one bit at a time, so for real use bitwise deniable encryption schemes are inefficient [7]. Here the mechanism of symmetric key encryption to encrypt the real data in which they apply symmetric data encryption key.

Decryption error problems contain in most deniable encryption schemes. These mistakes originate from the composed decryption mechanisms. For decryption it utilizes the subset decision mechanism. With the obtained subset decision result the receiver resolve the decrypted message. An error occurs when the element from the universal set is chosen by the sender; however unexpectedly the element is situated in the specific subset. In all translucent the same error occurs in the set-based deniable encryption scheme.

II. RELATED WORK

A. Fine grained Access control of Encrypted Data

Authors discussed that we need to encrypt data that are stored on sites in which many users share sensitive data and third party sites store information on Internet [2]. Data encryption can be specifically shared just at a coarse-grained level is one of the main disadvantages. To overcome this problem we introduce a new crypto system called Key-Policy Attribute-Based Encryption (KP-ABE) for fine-grained sharing of scrambled information. This technique shows that set of attributes can be a label for cipher text and to control which cipher texts a client can decode with access structure connected to private Keys. In order to share review-log information and broadcast encryption we need to illustrate the pertinence of our development. Hierarchical Identity-Based Encryption (HIBE) included in our development to support allocation of private keys [1].

B.Cipher text-Policy Attribute-Based Encryption

If a user possess a certain set of attributes then in several distributed environment only the user should access the data. Right now, the main technique for upholding such strategies is to utilize a server to store the information. In any case, if the server putting away the information is traded off, then the secrecy of the information will be bargained. Authors introduced a framework for acknowledging access control on encoded information that we call cipher text-policy attribute-based encryption [3]. By utilizing our strategies encoded information can be kept secret regardless of the fact that the capacity server is untrusted also, our techniques are secure against plot assaults.

Previous systems built policies into user's keys and used attributes to depict the encrypted data; while in our system encrypting data determines a policy for who can decrypt and the attributes are used to describe a user's credentials. Therefore, our techniques are theoretically nearer to customary access control strategies, for example, role-based access control (RBAC). Likewise, we give an execution of our framework and give execution estimations.

Drawback

- In use of linear secret sharing scheme and binary tree technique as the underlying tools authors introduced the cipher text policy attribute based encryption scheme with well-organized revocation.
- Authors demonstrated that the assigning capacity can be effectively given in the proposed plan, however every one of the representatives are connected with their unique delegator's one of a kind identifier.

C. Cipher Text Delegation for Attribute Based Encryption

Spurred by the topic of access control in the cloud storage, authors [5] considered the issue utilizing Attribute-Based Encryption (ABE) where clients' certifications may change and cipher texts might be put away by an outsider. We find that an extensive answer for our issue should at the same time take into account the repudiation of ABE private keys and in addition take into account the capacity to upgrade cipher texts to mirror the latest redesigns. Our fundamental result is gotten by matching two pledges:

Revocable Storage: We ask how an outsider can prepare a cipher text to preclude renounced clients from getting to information that was encoded previously, while the client still had entry. In applications, such capacity might be with an untrusted substance and all things considered, we require that the cipher text administration operations should be possible without access to any touchy information (which precludes unscrambling and re-encryption). We characterize the issue of revocable storage and give a completely secure development. Our center apparatus is another method that we call cipher text allocation. One can apply cipher text allocation on a cipher text scrambled under a specific access arrangement to're-encode' it to a more prohibitive approach utilizing just open data. We give a full investigation of the sorts of designation conceivable in various existing ABE plans.

Securing Newly Encrypted Data: We consider the issue of guaranteeing that recently encoded information is not decrypt able by a client's key if that client's access has been renounced. We give the primary technique for acquiring this disavowal property in a completely secure ABE plan. We give another and more straightforward way to deal with this issue has negligible adjustments to standard ABE. Authors recognize and characterize a basic property called piecewise key era which offers ascend to effective repudiation. We manufacture such answers for Key-Policy and Cipher text-Policy Attribute-Based Encryption by adjusting an existing ABE plan.

D. Deniable Encryption with Negligible Detection Probability

Deniable encryption, presented by authors [8], ensures that the sender or the recipient of a secret message can "fake" the message encoded in a particular cipher text in the nearness of a pressuring enemy, without the opponent distinguishing that he was not given the genuine message. To date, constructions are only known either for single-algorithm schemes with non-negligible detection probability or for debilitated variations with independent "honest" and "dishonest" encryption algorithms. Authors planned the first sender-deniable public key encryption system with negligible detection probability and a single encryption algorithm and portray a nonspecific intuitive development in light of an public key bit encryption scheme that has certain properties, and we give two illustrations of encryption schemes with these properties, one based on the quadratic residuosity assumption and the other on trapdoor permutations.

E. Sharing Files via Public-key Deniability

As cloud computing provides abundant registering assets, stockpiling, and transmission capacity to meet their processing needs, frequently at insignificant expense to users. All things considered administrations get to be admired and accessible to a bigger assortment of clients, security components turn into an essential piece of that[9]. Securing information for example, encryption, can shield correspondence and put away information from unapproved access including the administration supplier itself.

But, in way, many tools are not adequate against effective enemies who can force user to open the encrypted information. Authors proposed a new plan in this work which ensures security of data when the user communicates such plan and call it as deniable cloud storage. Here it shows that the problem cannot be adequately solved by any existing methods and frameworks. Besides, it provides an execution of deniable shared file system and use of practical aspects of user collaboration.

III. EXISTING WORK

The Data owner can insert how they need to share information regarding encryption is the principle idea of ABE. Explicitly, the one who satisfy the owner's conditions can effectively decrypt the stored data. The main feature of Attribute Based Encryption (ABE) is that it is not for users but only for those who have right to use. The data sharing plays a major role in cloud storage services so they utilize a very useful tool called ABE tool. To encrypt the data through pair wise keys is not practical by cloud storage users. In addition; it is likewise unfeasible to encode information repeatedly for some individuals.

The data owners can choose the type of users who can access their data and those who fulfill the conditions they can decrypt the cipher text [4]. The idea of deniable encryption is simple which is also like normal encryption schemes;

Deniable encryption has two separated schemes they are public key scheme and a deniable shared key. Our main effort and focus on the deniable public key encryption scheme in view of cloud storage scenario. The key generation functions and cipher text function provided by the public key system which is unaware.

Some of the disadvantages are computational overhead, flexibility of the coercion will be reduced due to the different encryption parameters for each encryption operation, simultaneously fully receiver deniable and the non-interactive schemes cannot be achieved and in non-committing schemes using one short key, it is impossible to encrypt unbounded messages.

IV. PROPOSED SYSTEM

The Storage services will be secure and error-free by implementing a deniable CP-ABE scheme on cloud. In all other deniable schemes, storage service providers are viewed like receivers within the above scenario in cloud. To implement deniability this work don't utilize public key systems which are simulatable or translucent sets like most previous deniable encryption schemes. At the same time two environments were built for encryption in Deniable Cipher Text Policy Attribute Based Encryption technique which is similar to the idea planned to it. Our plan with many dimensions while asserting there is only one dimension. This methodology eliminates clear excess parts. Replaced the Prime order groups through Composite order groups in existing ABE scheme.

The Prime order groups are faster than the Composite order groups in bilinear operation. To convert from the Composite order groups to Prime order groups there are a few strategies that can make good computational performance. For our deniable encryption work there may be a consistent environment provided by the Deniable Cipher Text Policy Attribute Based encryption. Instead of encrypting the data for multiple times, used single encryption work for all without updating the system. Do not consider the cipher text encryption whether the encryption is normal or deniable but this work should see the released receiver evidence ought to appear realistic for all cipher texts in this environment. The subgroup assignment provides the concept of deniability in the setup stage of system. Here, the decryption algorithm is deterministic that can be used by Deniable Cipher Text Policy Attribute Based Encryption.

To decrypt the normal cipher texts this work creates a suitable free fake key by the preventing property and the proper subgroup assignment. This plans do not have decryption errors in our scheme because decryption algorithm has been used which is still deterministic in our scheme. Figure 1 shows the system architecture and Figure 2 is the fake account page. Some of the advantages are there is no security violence, High Computational performance achieved and no data redundancy. In this work two algorithms used are Prime Order Bilinear Groups and Waters CP-ABE

A. Prime Order Bilinear Groups

In Composite order bilinear groups, the conversion in schemes based on pairs is equal to Prime order bilinear groups. This conversion can be used in cryptosystems based on pairs that make use of two properties like cancelling and projecting from composite-order bilinear groups. Our safety evidence pursues a diverse plan and utilizes only the projecting property. In prime-order bilinear groups, a new property that we call translating is used on behalf of cancelling property. The presence of translating property is not identified in composite-order bilinear groups but it acts a major role in the security proof. From basic reference string model, decisional linear assumption derives a scheme called blind signature that has two 2-move like round optimal and partial which is attained from the above proof with the own interest.

B. CP-ABE

In CP_ABE scheme by Sahai and Waters [4], if the user satisfy the owners condition and has a unique attributes then a user ought to just have the capacity to get to information. As of now, use of trusted server for information storage and arbitrate access control is the only method to impose the rule. Though, once the server compromised with the intruder to release the information then the confidentiality of the data will be gone. Cipher text-policy attribute-based encryption presents the system to realize that the encrypted data with complex access control in this paper.

Though with the untrusted storage server, the encoded information can be kept private by utilizing our systems; in addition, our techniques are secure against collision assault. Earlier attribute-based encryption systems construct policies into user's keys and depict the encrypted data with attributes; while in our framework party encoding information decides a strategy for who can decode and we use attributes to permit users access.

Hence the traditional access control techniques are conceptually closer to our concepts, for example, role based access control (RBAC). What's more, we give a system implementation and also execution estimations.

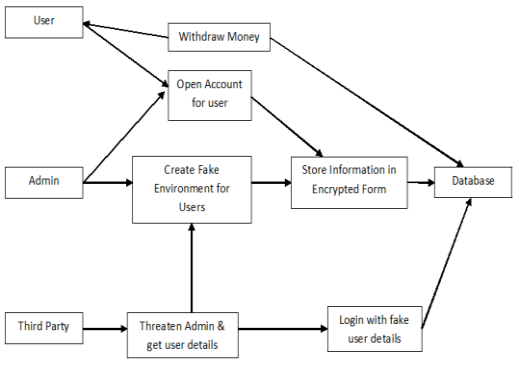

Figure 1: System Architecture

View Account :-

Username	rekha
Address	364313334443455467415
Email	3283133133643012023194473994314431954074554447
City	364313334443455467415
State	358301337325443451399411479
Phone No	364313334443455467415
Amount	200

Figure 2: Fake account page

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

V. CONCLUSION

In this paper, a CP-ABE scheme is implemented to provide secure data storage on cloud and error free storage service. Any intruder becomes invalid with the unique feature of deniability. The mechanism of fine grained access control assures that the data sharing is secure in ABE. The proposed work guarantees that any user can battle against wicked impedance by ensuring privacy of the user. Thus CP-ABE secures the privacy of user without any disclosure of information.

REFERENCES

1. Sahai, A., & Waters, B, Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2005, pp. 457-473.
2. Goyal, V., Pandey, O., Sahai, A., & Waters, B., Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89-98.
3. Bethencourt, J., Sahai, A., & Waters, B., Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, 2007, pp. 321-334.
4. Waters, B., Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *International Workshop on Public Key Cryptography*, 2011, pp. 53-70.
5. Sahai, A., Seyalioglu, H., & Waters, B.,Dynamic credentials and ciphertext delegation for attribute-based encryption. In *Advances in Cryptology–CRYPTO 2012*, pp. 199-217.
6. Hohenberger, S., & Waters, B., Attribute-based encryption with fast decryption. In *Public-Key Cryptography–PKC 2013*, pp. 162-179.
7. Tysowski, P. K., & Hasan, M. A., Hybrid attribute-and re-encryption-based key management for secure and scalable mobile applications in clouds. *IEEE Transactions on Cloud Computing*, *1*(2), 2013, 172-186.
8. Dürmuth, M., & Freeman, D. M, Deniable encryption with negligible detection probability: An interactive construction. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2011, pp. 610-626.
9. Gasti, P., Ateniese, G., & Blanton, M. ,Deniable cloud storage: sharing files via public-key deniability. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society, 2010*, pp. 31-42.

AUTHORS PROFILE

V**anitha M** holds a PhD in Computer Science and she is currently working as an Associate professor in VIT, Vellore. Her main area of interest is the study of machine learning techniques and developing the efficient VLSI architectures for cryptography algorithms. She has presented papers at conferences, published articles and papers in various journals.

Mangayarkarasi Ramaiah is an Associate professor in the School of Information Technology and Engineering at VIT University, Vellore, India. She has completed her Ph.D in the domain of computer vision. She has teaching experience of around fifteen years. Her area of specialisation includes computer vision, pattern recognition computer graphics and machine learning and she has published a number of research papers in international journals and International conferences.

Dr. Sumaiya Thaseen has thirteen years of teaching and research experience in VIT University. She completed her PhD in the domain of "Intrusion Detection Models using feature selection and ensemble of classifiers". She has publications in the domain of intrusion detection having good citations. She has more than ten publications in the domain of intrusion detection, few of which are indexed in Elsevier and SCI. According to Google Scholar, Sumaiya has over 249 citations and the H-Index is 8. Sumaiya is a reviewer for two Springer Journals.

J. Saira Banu is working as a faculty at School of Computing Science and Engineering, VIT University, Vellore. She completed her B.E. degree in Electrical and Electronics from Abdul Hakeem College of Engineering and Technology, Melvisharam, Tamil Nadu and completed her M.Tech and Ph.D in Computer Science and Engineering from VIT University. She has Eleven years of teaching experience. Currently she completed her research in parallel computing in multicores. Her areas of interest include parallel computing, computer architecture, Image Processing and Multicore Programming.