OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Secure and Efficient Privacy Preserving Provable Data Possession

TANAKALA BHARATH[1], S SURESH[2]
#1 M.Tech Scholar, Department of Computer Science Engineering,
#2 Associate Professor, Department of Computer Science and Engineering, Kakinada Institute of Engineering & Technology, Ap, India.

Abstract
Cloud Computing is a type of appropriated computing wherein assets and application stages are disseminated over the Internet through on request and pay on use premise. Many cloud storage encryption schemes have been acquainted with shield data from the individuals who don't approach. We make utilization of many schemes which accepted that cloud storage providers are protected and secure. Be that as it may, by and by, a few specialists (i.e., coercers) may attempt to uncover data from the cloud without the authorization of the data proprietor. In this paper, we exhibit that the location of obscurity clients with the utilization of our productive deniable encryption conspire, while the phony clients tries to get data from the cloud they will be furnished with some phony files. With the goal that programmers can't hack the files from the cloud. Also, they are happy with their copy record by that way we can secure the proprietor mystery files or confidential files.
Keywords: *Cloud computing, Deniable Encryption, Attribute Based Encryption, Data security and Privacy.*

I. Introduction

Cloud storage alludes to a cloud computing service model that stores data on remote servers. The data on remote servers is gotten to by means of the Internet or cloud. The servers are based on virtualization methods. Cloud storage is kept up, went down and oversaw by a cloud storage service supplier. Cloud storage providers are in charge of keeping the data accessible and available. Numerous organizations purchase or lease storage from the cloud providers to store their application data. This cloud storage services can be gotten to by web application programming interface (API) or by portable applications. Client data on cloud storage is scrambled utilizing distinctive encryption schemes to give assurance from gatecrashers [1]. Characteristic based encryption is a sort of open key encryption conspire in which the mystery key of a client and the produced ciphertext are dependent upon an arrangement of properties. In such a structure, the decoding of a ciphertext is conceivable just if the arrangement of traits of the client key matches the properties of the ciphertext. A focal security highlight of Attribute-Based Encryption is arrangement resistance. A conspiracy safe encryption calculation is the one in which two information sources don't hash to a similar yield. These schemes accept that the cloud providers don't uncover the cloud client's data and mysteries, which is not the reality dependably. For instance, in 2010, without informing its clients, Google discharged client archives to the FBI subsequent to accepting a court order [2]. In 2014, Edward Snowden unveiled the presence of worldwide observation programs that gather such cloud data as messages, messages, and voice messages from some innovation organizations [3], [4]. Once in a while unapproved client may likewise attempt to get to the data unlawfully. Keeping in mind the end goal to control unlawful access to cloud data, there is a requirement for deniable encryption service that denies illicit access to real data. This method was first proposed by R. Canetti et. al[5]. This encryption plot depends on polynomial deniability and creates a phony client data if the client is observed to be unapproved. The general thought of this deniable encryption conspire is to persuade the unapproved client by giving the phony data so the client does not endeavor to get to the data once more. Deniable encryption schemes don't model undertaking cloud data get to extremely well as far as client reaction time in light of the fact that the plan does not address reaction time necessities of clients of such frameworks. Subsequently another rank based deniable encryption conspire is proposed in this examination that tends to security and reaction time prerequisites of clients.

II. Related Work

The idea of ABE (Attribute-Based Encryption) in which data proprietors can embed how they need to appropriate data as far as encryption. That is, just the individuals who coordinate the proprietor's conditions can effectively unscramble put away data. We can state here that ABE is encryption for benefits, not for clients. This makes ABE an extremely accommodating apparatus for cloud storage services since data sharing is a critical

element for such services. Cloud storage clients are not commonsense for data proprietors to scramble their data by match astute keys. Moreover, it is additionally unreasonable to scramble data commonly for some individuals. With ABE, data proprietors settle on a choice just which sort of clients can get to their encoded data. Clients who persuade the conditions can unscramble the scrambled data. The plan of deniable encryption is only it additionally like basic encryption schemes, deniable encryption can be isolated into a deniable shared key plan and an open key plan. Permitting the cloud storage situation, we concentrate our endeavors on the deniable open key encryption plot. The simulatable open key framework gives an unconscious key era work and a neglectful figure content capacity. While exchanging an encoded bit, the sender will send an arrangement of scrambled data which might be normally scrambled or oblivious. Thusly, the dispatcher can guarantee some sent messages are unaware while really they are most certainly not. The plan can be connected to the collector side to such an extent that the plan is a bi-deniable plan. While playing out this plan there are a few drawbacks may emerge. Those are Computational overhead. I.e. Encryption parameters ought to be entirely unexpected for every encryption operation. So every intimidation will diminish adaptability. We can likewise confront Decrypted data with missing of substance at such pieces. Elements of the cloud condition may stop correspondences amongst clients and cloud storage providers and after that require storage providers to discharge client mysteries by utilizing power or different means. In this circumstance, encoded data are thought to be known and storage providers are asked for to release client insider facts here another impediment is Data repetition is Occur at each square of data. The non-intuitive and completely recipient deniable schemes can't be accomplished at the same time. It is likewise difficult to encode unbounded messages, utilizing one short key in non-submitting schemes. The future execution plot with Cipher Text Policy Attribute Based encryption shows a cloud storage supplier which intends to make counterfeit client insider facts. Determined such phony client insider facts, outside coercers can just got phony data from a client's put away figure content. The coercers think the got privileged insights are genuine, they will be substance and all the more unmistakably cloud storage providers won't have uncovered any genuine mysteries. In this way, client protection is as yet restricted in cloud computing environment[7].In request to defeat every one of these inconveniences Cipher content arrangement property based encryption (CP-ABE) plot is being actualized. The usage of a deniable CP-ABE conspire that can make cloud storage service. In these conditions, cloud storage service providers will simply look as recipients in other deniable schemes. Not at all like most past deniable encryption schemes, we don't utilize straightforward sets or simulatable open key frameworks to apply deniability. Deniable Cipher Text Policy Attribute Based Encryption conspire make with two encryption conditions in the meantime, much like the thought arranged in this plan with many sizes while guaranteeing there is just a single size. This approach expels clear excess parts. The base ABE plan can encode one piece each time; our deniable CPABE is unquestionably a square astute deniable encryption plot. The bilinear operation for the Composite request bunch is slower than the prime request gathering, there are a few strategies that can change an encryption plot from Composite request gatherings to prime request bunches for enhanced computational execution. Deniable Cipher Text Policy Attribute Based Encryption offers a dependable domain for our deniable encryption plot [8]. This plan expands a blending ABE, which has a deterministic decoding calculation

III. Methodology

Most of the deniable public key schemes are bit-wise, which means these schemes are able to method one bit a time. Hence, bit-wise deniable encryption schemes are in-competent for real use, particularly within the cloud storage service case. To solve this problem, considered a hybrid encryption scheme that concurrently uses even and asymmetric encryption they use a deniable encrypted plan-ahead even data encryption key, whereas real data are encrypted by a even key encryption mechanism. Mainly deniable encryption schemes are decryption error issues. These errors return from the considered decryption mechanisms. Uses the set decision mechanism for decryption the receiver decides the decrypt message according to the set call result. If the sender desires an element from the universal set however unluckily the element is located within the specific set, then an error occurs. The identical error happens in all clear set-based deniable encryption schemes. Scope the policy of a file may be unused to under the request by the client, when final the time of the agreement or totally move the files starting with one cloud then onto future cloud nature's domain. The position once any of the on top of criteria exists the policy is rejecting and the key director can totally withdraw from the public key of the associated file. So no one will develop the control key of a repudiated get in future. Because of this reason we will say the file is actually erased. To urge well the file, the user should invite the key controller to fabricate the public key for that the user should be verified. The key policy attribute based encryption standard is used for file access that is confirmed by means of an attribute connected with the file.

Deniable Encryption Process

Deniable encryption describe senders and receivers creating likely fake proof of fake data in cipher texts such that outside coercers are happy. Note that deniability comes from the reality that coercers cannot ensure the proposed facts is incorrect and as a result no reason to drop the given proof. This approach tries to overall block

coercion efforts since coercers understand that their efforts will be useless. We build use of this concept such that cloud storage providers can offer audit-free storage services. In the cloud storage situation, data owners who store their data on the cloud are just like senders within the deniable encryption scheme. Those that will access the encrypted data play the role of receiver within the deniable encryption theme, including the cloud storage providers themselves, who have system wide secrets and should be able to decode all encrypted data. We build use of ABE characteristics for securing stored data with an access control mechanism and deniable encryption to prevent outside auditing.

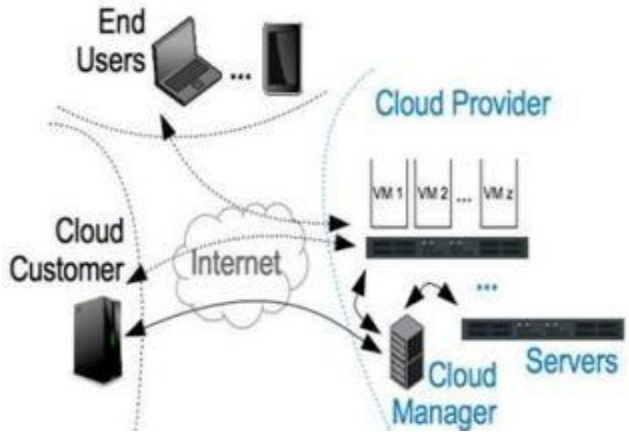

Figure 1: System Architecture

Composite order Bilinear Group

Design a deniable CP-ABE theme with Composite order bilinear teams for building audit-free cloud storage services. Composite order bilinear teams contain two attractive properties, namely projecting and cancelling. We build use of the cancelling property for building the same environment; on the other hand, freeman also known the important problem of computational value in regard to the Composite order bilinear group. The bilinear map operation of a Composite order bilinear group is far slower than the operation of a main order additive cluster with constant security level. That is, in this scheme, a user will pay out too much time in decryption once accessing files from the cloud. To make Composite order additive group schemes more realistic, into prime order schemes. Each sticking and cancelling cannot be simultaneously achieved in prime order teams in. For constant reason, we use a simulating tool projected to convert our Composite order bilinear group scheme to a main order bilinear group scheme. This tool is based on twin Ortho-normal bases and the subspace assumption. Not like subgroups are simulated as different Ortho-normal bases and so, by the orthogonal property, the bilinear operation is cancelled between different subgroups. Our formal deniable CP-ABE construction method uses only the cancelling property of the Composite order group.

Attribute-Based Encryption

Cloud storage services have quickly become more and more popular. Users will store their data on the cloud and access their data at any time. For the reason of user privacy, the data hold on the cloud is often encrypted and protected from access by other users. Considering the mutual property of the cloud data, attribute-based encryption (ABE) is considered one among the most suitable encryption schemes for cloud storage. There are many ABE schemes that are projected, including. Most of the proposed schemes assume cloud storage service providers or trusted third parties managing key management are trusty and cannot be hacked; yet, in follow, some entities could discontinue communications between users and cloud storage suppliers and then compel storage providers to release user secrets by using government power or other suggests that. in this case, encrypted data are understood to be known and storage Providers are requested to release their user secrets.

Cloud Storage

Cloud storage services have grown popularly. For the reason of the importance of privacy, several cloud storage encryption schemes are projected to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked. Still, in observe, some authorities (i.e., coercers) could force cloud storage providers to show user secrets or confidential data on the cloud, so in total circumventing storage encryption schemes. Here we gift a style for a new cloud storage encoding scheme that enables cloud storage providers to generate realistic fake user secrets to protect user privacy. As coercers cannot tell if obtained secrets are correct or not, the cloud storage providers make sure than user privacy remains firmly

protected. Most of the projected schemes guess cloud storage service providers or trusted third parties managing key management are trusted and cannot be hacked;

Distributed Key Policy Attribute Based Encryption

Key Policy-Attribute Based Encryption is a public key encryption primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for every of that a public key part is described. The encrypted or acquaintances the set of attributes to the message by contended with the comparing public key elements. Every client is assigned an access arrangement that is normally characterized as an access tree over information attributes. Client secret key is characterized to reproduce the access structure so the client has the ability to decipher a cipher-text if and simply if the information attributes fulfill his access structure.

IV. Proposed Methodology

In this work, it is describing a deniable ABE scheme for cloud storage services. By make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. This scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE) scheme. This enhance the Waters scheme from prime order bilinear groups to Composite order bilinear groups. By the subgroup decision problem assumption, this scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers. In this work, constructing a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, it is not using translucent sets table public key systems to implement deniability. Instead, this adopt the idea proposed with some improvements. This construct deniable encryption scheme through a multidimensional space. All data are encrypted into the multidimensional space. Only with the correct composition of dimensions is the original data obtainable. With false composition, cipher texts will be decrypted to predetermined fake data. The information defining the dimensions is kept secret. This make use of Composite order bilinear groups to construct the multidimensional space. This also use chameleon hash functions to make both true and fake messages convincing. In this work, there is a consistent environment for deniable encryption scheme. By consistent environment, means that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all cipher texts under this environment, regardless of whether a cipher text is normally encrypted or deniably encrypted. The deniability of this scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, can construct the released fake key to decrypt normal cipher texts correctly.

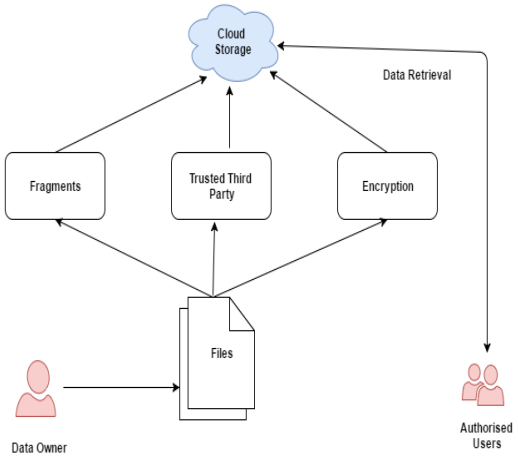

Fig 2: Proposed Architecture Diagram

V. Conclusion

In this work, we proposed a deniable CP-ABE scheme to build an audit-free cloud storage service. The deniability feature makes coercion invalid, and the ABE property ensures secure cloud data sharing with a fine-grained access control mechanism. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy. Cloud computing gives many advantages like storage security, increase storage space and reduce storage cost and decreases overheads on cloud, users. Proving the security to the data placed in cloud computing has become major issue in this IT platform. This paper mainly concentrates on security and privacy issues and also discusses about

the different techniques used in existing cloud environments. Further, these different techniques are used in improving the security of the data stored and also giving privacy to the data.

References

[1]. P. Mell and T.Grance, "The NIST Definition of Cloud Computing", Natinal Institute of Standards and Techology, vol. 53, no.6, pp. 1-3, 2009.

[2]. Leonard Heilig and Stefan Vob, "A Scientometric Analysis of Cloud Computing Literature", IEEE Transactions on Cloud Comouting, vol. 2, no. 3, pp. 266- 278, July-September 2014.

[3]. Cohen, Reuven, Rebello and Jagdish, "The State of Cloud Storage: A Benchmark Comparison of Speed, Availability and Scalability", White paper, Nausni, 2015.

[4]. J. J.Wylie, M. Bakkaloglu, V. Pandurangan, M.W. Bigrigg, S. Oguz, K. Tew, C. Williams, G. R. Ganger, and P. K. Khosla, "Selecting the Right Data Distribution Scheme for a Survivable Storage System", Carnegie Mellon University, Technical Report, May 2001.

[5]. Linlin Wu, Saurabh Kumar Garg, Steve Versteeg, and Rajkumar Buyya, "SLA-Based Resource Provisioning for Hosted Software-as-a-Service Applications in Cloud Computing Environments", IEEE Transactions on Services Computing, vol. 7, no. 3, pp. 465-485, JulySeptember 2014.

[6]. K. Hashizume, D. G. Rosado, E. Fernndez-Medina and E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, vol. 4, no. 1, pp. 1-13, 2013.

[7]. G. Kappes, A. Hatzieleftheriou and S. V. Anastasiadis, "Dike: Virtualization-Aware Access Control for Multitenant Filesystems", University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.

[8]. Srinivasa Rao Chintada, ChandraSekhar Chinta, "Dynamic Massive Data Storage Security Challenges in Cloud Computing Environments", International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 3, pp. 3609-3616, March 2014.

[9]. Kevin D Bowers, Ari. Juels and Alina Oprea, "HAIL: A High Availability and Integrity Layer for Cloud Storage", In the Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM, pp. 187-198, 2009.

[10]. Spillner J, Mller J and Schill A, "Creating Optimal Cloud Storage Systems", IEEE Transactions on Utility and Cloud Computing, vol. 29, issue. 4, pp. 1062-1072, June 2013.