ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 5, MAY 2015, PP 378-382

Augmented Privacy-Preserving Authentication Protocol by Trusted Third Party in Cloud

B.Sameena Begum, P.Ragha Vardhini

Abstract: Cloud management give well-mannered space for the clients to get delight from the on-demand cloud applications while not considering the local framework confinements. All through the data getting to, totally diverse clients is additionally in an exceptionally delightful relationship, thus learning sharing gets to be crucial to accomplish gainful edges. the common security measures essentially focus on the validation to comprehend that a client's privative learning can't be unapproved gotten to, however This paper concentrates on giving a trustworthy and secure cloud data sharing administration that permits clients element access to their data. Keeping in mind the end goal to accomplish this, we propose a compelling, versatile and adaptable security saving data strategy with semantic security; by using ciphertext policy attribute based encryption (CP-ABE) joined with identity-based encryption (IBE) methods despite guaranteeing strong data sharing security, our strategy succeeds in safeguarding the protection of cloud clients and backings proficient and secure element operations including, yet not restricted to, document creation, client denial and change of client characteristics. Security investigation shows that the proposed approach is secure under the nonexclusive bilinear gathering model in the arbitrary prophet model and upholds fine-grained access control, full conspiracy resistance and in reverse mystery. Moreover, execution examination and test results demonstrate that the overheads are as light as would be prudent.

Key words- CP-ABE, IBE, Dynamic operations, private key generator, Cloud Service Provider.

———————————— ◆ ————————————

I. INTRODUCTION

Cloud computing is that the delivery of computing and storage capability as a service to a heterogeneous community of end-recipients. Cloud computing could be a general term for love or money that involves delivering hosted services over the web. A model for delivering data technology services during which resources square measure retrieved from the web through web-based tools and applications.Putting away data in the cloud offers clients the accommodation of access without obliging direct learning of the sending and administration of the equipment or framework. Despite the fact that Cloud computing is significantly more effective than individualized computing, it brings new protection and security challenges, as clients give up control by outsourcing their data they no more having physical ownership of it. By having full access to cloud administrations, clients' data are presented to a mixture of dangers and vindictive assaults and instances of security ruptures happen often (Arrington, 2006). Case in point, a few mists may be unfaithful to data privacy for money related reasons; classified data may be revealed to business contenders; or the CSP may disguise data misfortune to keep up their notoriety (Shah et al., 2007). In outline, in spite of the fact that Cloud computing is financially appealing to purchasers and endeavors by offering clients huge scale data sharing, it doesn't promise clients security and data security. Data proprietors request abnormal amounts of security and privacy when they outsource their data to a cloud; in spite of the fact that they typically scramble their data when putting away it in a cloud server, they stillwant control over it, for instance, in the event that they much of the time upgrade it (Erway et al., 2009; Ateniese et al., 2008). Direct occupation of customary cryptographic primitives can't accomplish the data security needed. In this manner, a lot of work has as of late been coordinated towards guaranteeing the security and security of remotely put away shared data utilizing a mixture of frameworks and security models (Yu et al., 2010a; Wang et al., 2010). These have basically centered around protecting clients' protection while acknowledging wanted security objectives, without presenting unreasonably abnormal amounts of many-sided quality to the clients at the decoding stage. To understand these issues, scientists have either used key-policy attribute-based encryption (KP-ABE) for secure access control or utilized hierarchical identity-based encryption (HIBE) for data security. Yu et al. (2010a) were the first group to accomplish secure data access control with provable security in Cloud computing utilizing KP-ABE. Be that as it may, by uncovering a percentage of the clients' ascribes to cloud, these frameworks were not able to completely safeguard clients' protection. Then again, the HIBE-based plan (Wang et al., 2010) uses progressive encryption to guarantee data security in a cloud, however this presents an excess of private keys for every client to be overseen effectively.

In outline, these plans either have security blemishes or give security to the detriment of execution; accordingly, the test of accomplishing the double objectives of protection safeguarding with powerful cloud

- ***B.Sameena Begum*** *is currently pursuing master's degree program in computer science & engineering in Ravindra College of Engineering for Women(JNTUA), India,***E-mail: b.sameena2012@gmail.com***

P.Ragha Vardhani,*.Currently she is working as Assistant Professor in Department of Computer Science Engineering in Ravindra College of Engineering for Women, Kurnool. India,* ***E-mail: ragha.vardhani@gmail.com***

data sharing stays uncertain. To understand a compelling, adaptable and security safeguarding data sharing administration in Cloud computing, the accompanying difficulties need to be met: firstly, data proprietors ought to have the capacity to allot other cloud clients with diverse access benefits to their data; also, the cloud needs to have the capacity to bolster element asks for so that data proprietors can add or renounce access benefits to different clients permitting them to make or erase their data; thirdly, the clients' protection must be secured against the cloud so they can hide their private data while getting to the cloud; at long last, clients ought to have the capacity to get to shared data in the cloud through joined innovations with low figuring capacity, for example, cell phones and tablets. To date, illuminating these critical ranges in Cloud computing stays slippery. In this paper, we propose a viable, versatile and adaptable protection protecting data sharing plan in the cloud that guarantees both semantic security and successful accessibility of client data. To safeguard protection and insurance data classifiedness against the cloud, the plan utilizes a cryptographic primitive, named cipher-text policy attribute-based encryption (CP-ABE) and consolidates it with a personality based encryption (IBE) procedure; every data document is portrayed by a situated of important traits, permitting every client to be allocated an entrance structure that characterizes the extent of data documents they can have admittance to. To implement these entrance structures, this plan characterizes an open private key pair for every property. For every client' mystery key, it is a mix of client's ID (i.e., client's open key) and the characteristic's mystery key, subsequently guaranteeing that every quality displays an alternate key to every client. Data records are scrambled by open key parts and access networks changed over from the entrance structure; client mystery keys are characterized to mirror their entrance benefits so that a client can just unscramble a ciphertext on the off chance that they have the coordinated credits to fulfill the ciphertext. To determine the testing issues of intrigue resistance, our plan furnishes clients with an open key fitted to their mystery keys; we utilize client's ID (open key) to "tie" together the credits fitting in with this client so that they can't be effectively joined with another's client's characteristics.

To secure client security, our plan does not have to overhaul client mystery key with the goal that it avoids cloud access client access structure. To lessen the key administration issue, the data proprietor basically allots mystery keys to clients through the cloud. Contrasted with past plans, our proposed plan gives the advantages of security and effectiveness: 1) the cloud can learn nothing around a client's protection or access structure, thusly the plan is completely intrigue safe; 2) every developed operation, including client repudiation, can just influence the present document or client without including key upgrades. Subsequently, the primary commitments of this paper can be abridged as takes after:

1. Our plan proposes successful, adaptable encryption for a cloud data sharing administration that all the while accomplishes full protection protecting, arrangement resistance and data privacy.

2. We demonstrate that the proposed plan gives semantic security to data partaking in Cloud computing through the arbitrary prophet under the non specific bilinear gathering model (Boneh et al., 2005). Moreover, our plan all the while implements fine-grandness, in reverse mystery and access benefit privacy.

3. The execution examination shows that our plan just acquires a little overhead contrasted with existing plans; in the interim, the test results exhibit that the overheads are as light as would be prudent.

II. RELATED WORK:

CLOUD SERVICES Data privacy a lot of study has been done on the potential of cloud and the services that cloud computing can and could deal. These services can be characterized into four main sections: Storage as a Service (StaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Following section highlights these services and their usage in depth.

A. STORAGE AS A SERVICE

Cloud offers a storage space that is huge, seemingly boundless, and rising every day. Storage as a Service (StaaS) allows cloud applications to gauge beyond their inadequate servers. Cloud storage systems needs to focus on requirements for upholding users' data and data, considering high performance, availability, replication, data reliability and reliability. The accountability to individual is maintained and upholds customer’s own computer storage as cloud vendors deal them the choice of loading their data in the cloud which is reachable whenever they need [11]. Unfortunately, due to the contradictory nature of the necessities of cloud services, no one system implements all of them together.

B. SECURITY ISSUES

Companies are promptly moving onto cloud because they can now use the greatest capitals available on the market in the blink of an eye and also decrease their operations’ cost radically. But as more and more data is moved to the cloud the security concerns have continuing to grow. Data breaking is the biggest security issue. A capable hacker can easily get into a client side application and get into the client’s intimate data [2].Incompetent and faulty APIs and interfaces become the target. IT companies which provide cloud services allow third party companies to alter the APIs and familiarize their own functionality which in turn allows these companies to comprehend the internal workings of the cloud[2].Denial of Service (DoS) is also a major menace wherein the user is approved partial or not at all access to their data. Companies now use cloud very frequently say all days and DoS can root huge increase in cost both for the user and service provider. Connection snooping is that in which a hacker can scan your online actions and copy/replay a particular broadcast to get into your private data. It can also lead to the user to unlawful or unsolicited sites. Data loss is also another issue. A malicious hacker can wipe out the data or any natural/man-made disaster can destroy your data. In such cases having an offline copy is a big advantage. Carelessness of the service provider can also lead to data loss [3].Compatibility between different cloud services is also an issue. If a user decides to move from one cloud to another the compatibility ensures that there is no loss of data. Cloud can also be used for wrong purposes i.e. cloud abuse. Due to the availability of latest technologies on the cloud it can be used for high end calculations which cannot be done on a standard computer [2],[3].Insufficient understanding of cloud technologies can lead to unknown levels of risk. Companies move to cloud because it provides substantial reduction in cost but if transfer is done without proper background learning, the problems that arise can be even greater. Internal intruders are able to use the data for harmful purposes. Safe storage of encryption keys is also a problem. Even if you are using encryption for enhanced security, keeping a key a safe asset becomes an issue. Who should be the owner of the key? User seems to be the answer but how diligent and careful can he/she be will decide the security of the data.

III. PROBLEM STATEMENT

3.1. SYSTEM MODEL

Our framework model, as indicated in Fig. 1, requires four gatherings in a system: The data proprietor; who has data put away in the cloud and relies on upon the cloud for data support. Data proprietor can be undertakings or individual clients. The data shopper; who gets to the data shared by the data proprietor, downloads data of interest and unscrambles it utilizing his mystery keys (for curtness, data customers are alluded to as clients in this paper). The cloud server (CS); gives a top notch administration using various servers with significant storage room and calculation power. The private key generator (PKG); is a trusted outsider that registers relating private keys for clients (Boneh and Franklin, 2001). In our framework, the PKG is just tasked with conveying open keys to the data proprietor and to produce and convey comparing private keys to the clients, as portrayed by Roosters (2001). Since there is no motivation to uncover data to the PKG, private data is kept separate from the PKG and no other security issues are exchanged to the PKG. Also, the data proprietor stores his data in an arrangement of cloud servers which are running in a participated and Cloud way; subsequently, the data proprietor can interface with the cloud servers to alterably get to and overhaul his data through the CS supplier (CSP). Also, the CS needs to dependably be online; though, data proprietors and buyers can be logged off.

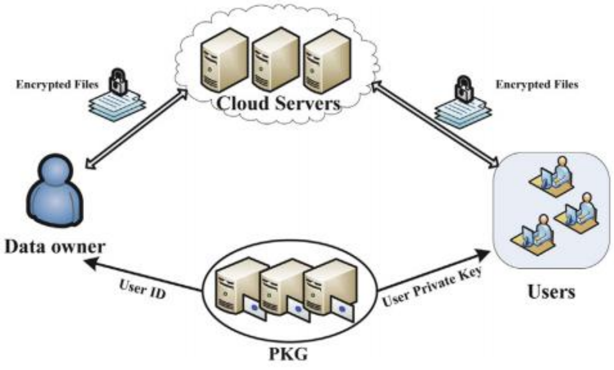

Fig1. System model

3.2. ADVERSARY MODEL

The adversary model considers most threats to cloud data confidentiality as malicious. In contrast, the CS in our model is semi-trusted (also known as passive), in that it behaves appropriately most of time; however, in certain situations an entity may arbitrarily deviate from the protocol specifications and the CS may try to acquire as much secret data as possible (De Capitani di Vimercati et al., 2007). We suggest that although the semi-trusted adversary model is weaker than the malicious model, it is often a more realistic model. The three types of threats can be categorized as follows: 1. Inner threats (from the CSP and users who might obtain unauthorized data), and outer threats (from unauthorized attackers and external adversaries beyond the system domain). 2. Active attacks (where unauthorized users inject malicious files into the cloud), and passive attacks (where unauthorized users eavesdrop on conversations between users and the cloud). 3. Collusion between the CSP and users (to access unauthorized data for the purpose of harvesting file contents).

3.3. SECURITY REQUIREMENTS

With respect to secure data sharing and data access control in the cloud, the main goal of our model is to protect the cloud data from being accessed by inner intruders, including With respect to secure data sharing and data access control in the cloud, the main goal of our model is to protect the cloud data from being accessed by inner intruders, including the cloud and from external attackers and unauthorized outer users. As such, our system has the following requirements: 1. Fine-grained access control: each user should only be able to access the data they are allowed to, with no access to unauthorized data. 2. Collusion resistance: users should not be able to collude with any other user, or the cloud, for the purpose of sharing their secret key to access unauthorized data. 3. Backward secrecy: the data access control policy should have the functionality to ensure that users are unable to access cloud data once their privileges have been revoked.

3.4. DESIGN GOALS

The main design goals of our system are as follows: provide an adversary model, as previously described, with a secure, private and scalable policy for data sharing in cloud computing. As such, data owners are required to assign access structures to define which files users are allowed access, by generating unique key combinations for each attribute that are specific to each user; to protect users' privacy against the CS, by prohibiting the CS from learning the contents of user data or data on users' access privileges; to support dynamic user requests, such as addition and revocation of user access privileges; finally, the ensure the overheads of the service provided by the system are as light as possible.

IV.THE PROPOSED SCHEME

In order to improve privacy and security for data sharing in cloud computing, we propose a scheme that combines CP-ABE (Bethencourt et al., 2007) and IBE (Shamir, 1985). Based on ABE, we choose two random exponents for every attribute, while the proposed scheme introduces a hash function that maps user IDs to group elements in the algorithm of key generation and decryption

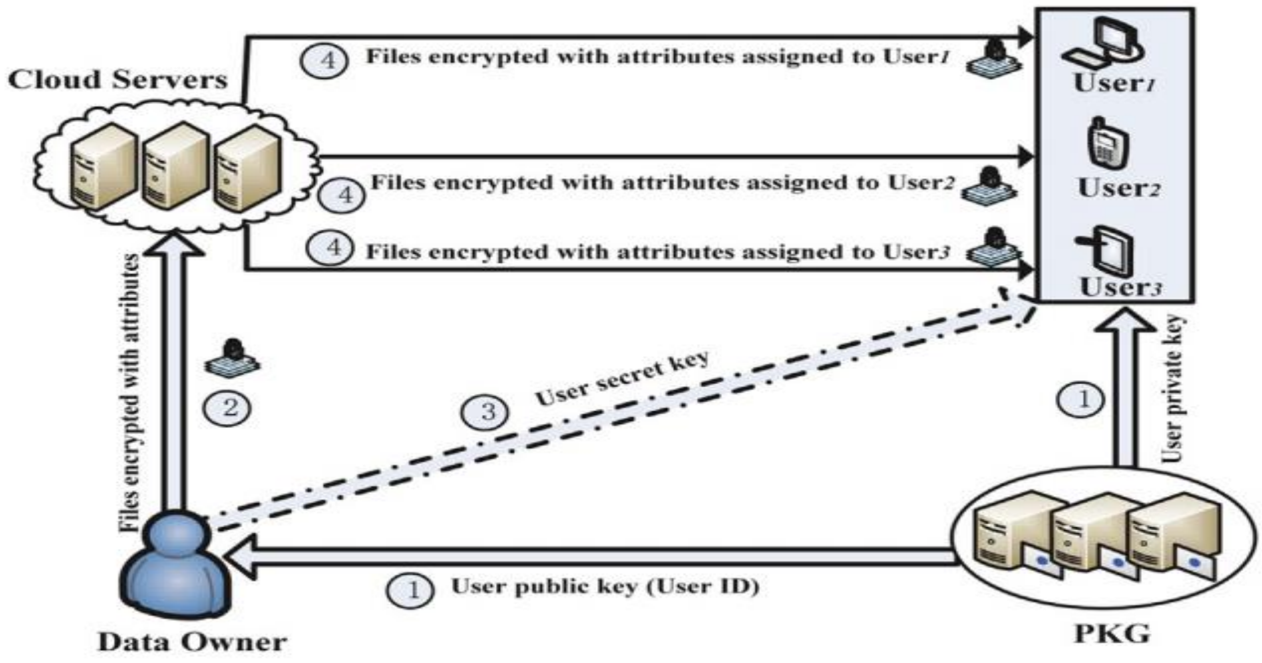
Cloud Servers
4 Files encrypted with attributes assigned to User1
User1
4 Files encrypted with attributes assigned to User2
User2
4 Files encrypted with attributes assigned to User3
User3
Files encrypted with attributes
2
3 User secret key
1 User private key
1 User public key (User ID)
Data Owner
PKG

Fig 2. Proposed System Architecture

4.1. OVERVIEW

Our scheme is based on a bilinear map. Let G1 and G2 be two cyclic groups of prime order q, and g1 is the generator of group G1. A bilinear map e : G1 G1/G2 satisfies the following properties:

1. Bilinearity: for all y; z˛G1 and a,b ˛ Zq, where Zq ¼ {0,1,2,..q 1}, we have e(ya ,zb)¼e(y,z) ab.

2. Computability: for any y; z˛G1, there is a polynomial time algorithm to compute eðy; zÞ˛G2.

3. Non-degeneracy: e(g1,g1) s 1.

Similar to CP-ABE (Waters, 2011), each file is described by a set of attributes. Determined by the set of attributes that a file has, an access tree is assigned to the file. The access tree is converted to a Linear Secret Sharing Scheme (LSSS) matrix (Beimel, 1996). Each user has a set of attributes given by the Fig. 1 e System model. data owner and owns a unique ID regarded as his public key.

For each attribute the user has, a key for the user ID is created. A user is able to decrypt the data in the cloud server if and only if he has a matched set of attributes. In addition, there exists a user list (UL) in the cloud to retain the authorized user IDs (public keys) in our system. The proposed scheme elegantly integrates four randomized algorithms: System initialization, Encryption, Key generation, Decryption to achieve effective, scalable and privacy preserving cloud data sharing service. Fig. 2 describes a simplified workflow of the proposed scheme. At the initialization phase, the data owner uses the System initialization algorithm to generate system parameters for all system entities. The data owner then employs Encryption algorithm to encrypt files with “attributes” and uploads to the cloud. By the Key generation algorithm, the data owner generates secret keys for each user, and then delivers them to the users via the cloud server. At last, users use Decryption algorithm to decrypt ciphertext if their attribute set matches with the file attributes. In the following subsection

V.CONCLUSION

In this paper, we introduce privacy-preserving and secure data sharing scheme in cloud computing by abusing CPABE and consolidating it with system of IBE. The proposed plan guarantees fine-grained data access control, in reverse mystery and security against conspiracy of clients with the cloud and backings client expansion, renouncement and trait changes which are not gave by current works. Besides, our plan does not uncover any credit of clients to the cloud so that keeps the security of the clients far from the cloud. Security investigation demonstrates that the proposed plan is semantically security in the bland bilinear gathering model, demonstrating H as an arbitrary prophet. Also, we assess the execution of the proposed plan about processing intricacy, correspondence expense and ciphertext size. The outcome demonstrates that the proposed plan is low overhead and very proficient. Taking after the ebb and flow research, we will execute the proposed protection saving and viable cloud data sharing administration in a genuine CSP stage for future work.

REFERENCES

1] H. Y. Lin and W. G. Tzeng, “A Secure Erasure Code-Based CloudStorage System with Secure Data Forwarding,” IEEE Transactions on Parallel and Cloud Systems, vol. 23, no. 6, pp. 995-1003, 2012. [2] I. T. Lien, Y. H. Lin, J. R. Shieh, and J. L. Wu, “A Novel Privacy Preserving Location-Based Service Protocol with Secret Circular Shift for K-nn Search,” IEEE Transactions on Data Forensics and Security, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6476 681, 2013.

[3] R. S´anchez, F. Almenares, P. Arias, D. D´ıazS´anchez, and A.Mar´ın, “Enhancing Privacy and Dynamic Federation in IdM foR Consumer Cloud Computing,” IEEE Transactions on ConsumerElectronics, vol. 58, no. 1, pp. 95-103, 2012.

[4] Y. Tang, P. C. Lee, J. C. S. Lui, and R. Perlman, “Secure Overlay Cloud Storage with Access Control and Assured Deletion,” IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 903-916, 2012.

[5] A. Mishra, R. Jain, and A. Durresi, “Cloud Computing: Networking and Communication Challenges,” IEEE Communications Magazine, vol. 50, no. 9, pp, 24-25, 2012.

[6] J. Chen, Y. Wang, and X. Wang, “On-Demand Security Architecture for Cloud Computing,” Computer, vol. 45, no. 7, pp. 73-78,2012 .

[7] H. Wang, “Proxy Provable Data Possession in Public Clouds,”IEEE Transactions on Services Computing, [online] ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnu mber=6357181, 2012.

[8] L. A. Dunning and R. Kresman, “Privacy Preserving Data Sharing With Anonymous ID Assignment,” IEEE Transactions on Data Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Transactions on Parallel and Cloud Systems,vol. 22, no. 5, pp. 847-859, 2011.

[10]Y. Zhu, H. Hu, G. Ahn, and M. Yu, “Cooperative Provable DataPossession for Integrity Verification in Multi-cloud Storage,” IEEE Transactions on Parallel and Cloud Systems, vol. 23, no, 12, pp. 2231-2244, 2012.

ABUT AUTHORS

B.Sameena Begum,Pursuing M.Tech (CSE) from Ravindra College of Engineering for Women(JNTUA). Research area of interest includes Cloud Computing, Computer networks.

Mrs. P.RAGHA VARDHANI, received B.Tech (CSE) degree from Vaagdevi Institute of Technology & Science and M.Tech (CSE) from Vaagdevi Institute of Technology & Science. Currently she is working as Assistant Professor in Department of Computer Science and Engineering in Ravindra college of Engineering for Women, Kurnool. She has lifetime membership in Indian Institute of Technical Education (ISTE).