AMSE Association for the Advancement of Modelling & Simulation Techniques in Enterprises
IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Advances in Modelling and Analysis B
Vol. 61, No. 2, June, 2018, pp. 106-112
Journal homepage:http://iieta.org/Journals/AMA/AMA_B

A novel key management mechanism using elliptic and Diffie-Hellman for handling users in cloud environment

K. Santhi Sri[1*], N. Veeranjaneyulu[2]

[1] Department of CSE, Vignan's Foundation for Science Technology & Research, Vadlamudi, Guntur 522213, Andhra Pradesh, India
[2] Department of IT, Vignan's Foundation for Science Technology & Research, Vadlamudi, Guntur 522213, Andhra Pradesh, India

Corresponding Author Email: srisanthi@gmail.com

https://doi.org/10.18280/ama_b.610209

Received: 17 April 2018
Accepted: 5 June 2018

Keywords:
cloud computing, elliptic curve, data owner, cloud user, data storage

ABSTRACT

Cloud computing provides many number of services to the users but the major and crucial service is cloud storage. Cloud storage is one of the most popular services in cloud computing environment. But the data stored in cloud will have a problem of protecting the data from the third party and also address the unauthorized access. For solving such issues encryption provides a better solution but access given to the cloud users is a problem. In order to address this problem we propose a group key management technique using Diffie-Hellman and elliptic curve cryptograph. Which handles the user authentication and also give the group access, and role based access to the user.

1. INTRODUCTION

There has been a creating model in the present conditions to store data in the cloud with the enthusiastic addition in the measure of cutting edge data, for instance, customers' near and dear data to greater activities expecting to go down databases or store recorded data. Cloud data storing can be particularly engaging for customers with sporadic limit demands, requiring an unassuming accumulating level or a negligible exertion, whole deal record. By outsourcing customers' data to the cloud, authority communities can focus more on the diagram of abilities to upgrade customer experience of their organizations without worrying over resources for store the creating measure of data. Cloud can moreover give on ask for advantages for limit which can assist master associations with decreasing their help costs. In addition, disseminated capacity can give a versatile and supportive way forClients to catch their information from anyplace on any device. In any case, a few late reviews [1-2] demonstrate that 88% potential cloud buyers are stressed over the protection of their information, and Security is regularly referred to as the best deterrent for cloud reception. There are diverse sorts of Infrastructures related with a cloud [3]. An open cloud is a cloud which is made accessible to the general people, and assets are controlled in a compensation as-you-go way. A private cloud is an inside cloud that is gathered and worked by a solitary connection. The connection has full control of the private cloud, and the private cloud can't be developed to by outside parties. Consequently a private cloud is routinely thought to be more secure and trusted.A current review [4] demonstrates that almost half, 43% of all organizations report using private mists and 34% of organizations say they will start to utilize some type of private cloud in the following six to a year.In this paper, we address the issue of secure data storage of individuals by a large cloud. Open cloud is confined by no less than one server cultivates consistently passed on topographically in different territories. Customers don't know where their data is secured and there is a strong perception that customers have lost control over their data after it is exchanged to the cloud. To empower customers to control the passage to their data set away in an open cloud, sensible access control courses of action and frameworks are required. The passage systems must farthest point data access to only those arranged by the data proprietors. These methodologies ought to be approved by the cloud. In various current dispersed stockpiling structures, data proprietors need to acknowledge that the cloud providers are trusted to keep unapproved customers from getting to their data.

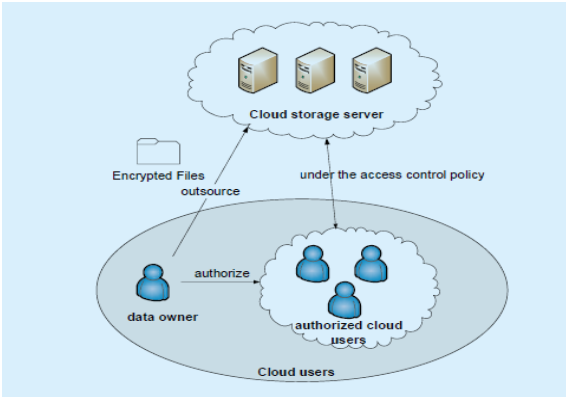

Figure 1. Cloud storage architecture

In role based access control (RBAC) demonstrate, parts are mapped to get to consents and clients are mapped to proper parts. For example, clients are doled out participation to the parts in view of their duties and capabilities in the association. Authorizations are allocated to qualified parts rather than

singular clients. Besides, in RBAC, a part can acquire consents from different portions, thus there is a various level structure of parts. Since being first formalized in 1990's, RBAC has been generally utilized as a part of numerous frameworks to furnish clients with adaptable access control administration, as it permits get to control to be overseen at a level that compares intently to the association's arrangement and structure.

In this paper, we propose a novel group key administration calculation in view of elliptic bend and Diffie-Hellman. We plan a protection saved distributed storage framework system, in view of which we characterize the security dangers to the cloud information. We propose a gathering key administration calculation for the scrambled cloud information offering to the dynamic gathering. The plan is actualized in light of the calculation and does not rely upon any trusted substance or the security impart.

1.1 Cryptographic key management overview

In this area, we audit the two general classes of cryptographic keys, list the most normally utilized key writes, recognize the key states and graph the subsequent progress outline. We at this point depict the most critical key administration capacities (likewise alluded to as key lifecycle activities) and rundown the nonspecific security necessities related with these capacities.

1.2 Key types

Cryptographic keys fall into two general classifications:

1. **Secret key**: A key that is by and large used to 1) perform encryption/decoding utilizing symmetric cryptographic calculations; as well as 2) to give information trustworthiness utilizing message validation codes or an encryption method of task that additionally gives information uprightness. A mystery key is additionally called a symmetric key, since a similar key is required for encryption and unscrambling or for trustworthiness esteem age and uprightness confirmation.

2. **Public/Private Key Pair**: A couple of scientifically related keys utilized as a part of private, public key cryptography for confirmation, computerized mark, or key foundation. As the name demonstrates, the private key is utilized by the proprietor of the key match, is kept mystery, and ought to be ensured constantly, while the general population key can be distributed and utilized be the depending gathering to finish the convention or upset the tasks performed with the private key.

From these general classifications one can decide the most regularly utilized key composes in a distributed computing condition. It is not necessarily the case that a cloud execution might not have extra kinds of keys.

1. **Public/Private Authentication Key Pair**: This key match is utilized by one gathering to validate to the next gathering. Its run of the mill utilize involves consolidating an arbitrary test with the endorser produced irregular number and marking the outcome for the advantage of the challenger who wishes to confirm the private-key holder. Cases of utilization incorporate customer validated Transport Layer Security, Virtual Private Network confirmation, and keen card-based logon. A confirmation key match is for the most part utilized as a part of a system situation and is by and large utilized for long haul utilize.

2. **Public/Private Signature Key Pair**: The private key of the key match is used by one social event to deliberately sign a message/data, while the relating open key is used to affirm the stamp. Instances of the use of a check key join are stamped Secure/Multipart Internet Mail Extensions messages, stamped electronic chronicles, and stamped code. In a few executions, a key match might be utilized for both verification and mark capacities. A mark key match is by and large utilized as a part of a system domain and is for the most part utilized for long haul utilize. It might likewise be utilized to produce and check marks on put away information.

3. **Public/Private Key Establishment Pair**: This key match is utilized to safely build up a key between parties. Cases of the utilization of a key match for key foundation are encoding the symmetric key for S/MIME payload encryption/decoding and scrambling the irregular mystery to be sent from a TLS customer to a server. It is suggested that key foundation key sets be unmistakable from validation and mark key sets. In any case, it is perceived that a few gadgets, for example, web servers utilize a similar key match for key foundation and validation. A key foundation key match is generally utilized as a part of a system domain, yet some use for put away information is likewise observed and can be imagined. A key foundation key match is for the most part utilized for a pre-characterized period for encryption (e.g., up to 3 years), yet is utilized for unscrambling for whatever length of time that the classification of the information should be ensured.

4. **Symmetric Encryption/Decryption Key**: A symmetric key is utilized to scramble and decode information or messages. For information in-travel, a symmetric encryption/decoding key may have a short life, commonly for each message (e.g., S/MIME message) or for every session (for instance a TLS session). For put away information, the symmetric existence of the encryption/decoding key has a tendency to be the length of the classification of the information should be secured.

5. **Symmetric Message Authentication Code Key**: A symmetric key is utilized to give confirmation to the trustworthiness of information.

6. Symmetric Key Wrapping Key: A symmetric key is used to scramble a symmetric key or private key. A Key Wrapping Key is also called a Key Encrypting Key.

1.3 Different states of the key

A symmetric key or open/private key consolidate can encounter the going with states. It isn't really the case that a key organization execution won't not have additional states. Of course, a key organization execution may have a subset of these states.

• Generation: A symmetric key or open/private key match is made when required.

• Activation: A symmetric key or private key is sanctioned when it is required to be used. An open key is activated when it is made available or on the date exhibited in its related metadata.

• Deactivation: A symmetric key or private key is deactivated when it is never again required for applying cryptographic confirmation to data. Deactivation of these keys may be trailed by devastation or archived. An open key isn't deactivated. It may end

• Suspension: A key may be suspended from use for a combination of reasons, for instance, a dark status of the key or due to the key proprietor being quickly away. Because of individuals when all is said in done key, suspension of the

sidekick private key is passed on to the depending parties. This may be granted as an "On hold" disavowal reason code in a CRL and in an Online Certificate Status Protocol (OCSP) response

• Expiration: A key may slip by in view of the complete of its crypto period [refer RFC 4949]. By virtue of an open key, an end date is appeared in the related metadata.

• Destruction: A key is pulverized when it is never again required.

• **Archival**: A key might be chronicled when it is never again required for typical utilize, however might be required after the key's crypto period. A case for mystery or private keys is the conceivable decoding of chronicled information. A case for open keys is the check of chronicled marked archives.

• **Revocation**: A repudiation is expressly expressed as for open keys; be that as it may, the disavowal likewise applies to the relating private key. Renouncement data is safely conveyed to the depending parties, for instance, as CRLs or OCSP reactions, on account of X.509 open key testaments. Mystery keys are additionally "denied", regularly by including them on records, for example, a traded off key rundown.

1.4 Key management - generic security requirements

The following are general key administration security prerequisites:

1. Gatherings performing key administration capacities are legitimately validated and their approvals to play out the key administration capacities for a given key are appropriately confirmed.
2. All key administration orders and related information are shielded from imitating, i.e., source verification is performed earlier executing a sum on.
3. All key administration charges and related information are shielded from undetected, unapproved alterations, i.e., trustworthiness security is given.
4. Mystery and private keys are shielded from unapproved exposure.
5. All keys and metadata are shielded from parodying, i.e., source confirmation is performed before getting to keys and metadata.
6. All keys and metadata are shielded from undetected, unapproved adjustments, i.e., uprightness insurance is given.
7. At the point when cryptography is utilized as an assurance component for any of the over, the security quality of the cryptographic system utilized is in any event as solid as the security quality required for the keys being overseen.

2. LITERATURE SURVEY

Nabeel et al. familiar an achievable course of action with meet various impediments in light of the all-inclusive community key cryptosystem [15]. In rapidly, the beforehand specified works simply consider a specific circumstance. With the ascent of web of things (IoT), the security threats have drawn extending thought. To suit various conditions and higher necessities (acted by the rational applications) to PS structure, distinctive countermeasures were proposed, for instance, [9] and. Meanwhile, to light up the consistently creating security threats of PS system in new conditions, different plans were similarly proposed.

Diro et al. proposed a lightweight arrangement by using elliptic twist cryptography to ensure security in dimness based PS structure [20]. A sheltered PS system that gives customer data security by using different leveled inside thing encryption was proposed by Rajan et al. [21].

Beligianni et al. presented an answer that defended purchaser security in astute networks [22]. As a result of the brain boggling condition, more sensible courses of action ought to be abused. Additionally, the security perils, (for instance, the assention ambush) still need to pay more contemplations [13]. The differential assurance advancement is a fitting other option to guarantee fog based PS structure security. Thriving with the advancement of enormous data and IoT, differential insurance transforms into a hot area of research [19, 28–31].

Dwork and Roth analyzed the differentially private procedures for instrument diagram and machine learning in [28]. Dwork kept an eye on the importance of differential insurance and gave an examination to the differential security backwoods [29].

An arrangement based approval conspire [24] which can be keep running as an Infrastructure as a Service display with a specific end goal to secure the clients security by guaranteeing that they can set their own particular protection approaches so as to shield the client information from unapproved get to. The OASIS cloud approval [25] has arrangements for the administration of approvals in the cloud benefit conveyance models. It keeps up a log of where the clients are and the points of interest of the gadgets that are being utilized by them.

Dell [27] information security/encryption has took into account ensuring the different client information that is being put away on an outer drive or media. Programming and equipment based encryption plans are conveyed. The fundamental favourable position being that the client intercession isn't required to authorize strategies and they are anything but difficult to convey and oversee also. Dell additionally has utilized the Transparent File Encryption in which a control over the different clients getting to the information is kept up. In this strategy a white rundown of clients are made will's identity given the entrance to administrations and to share records. The checking of the use, examining of occasions and report creation and the workload of the consistence is likewise diminished.

The Wuala cloud [28] accommodates the encryption of information in PCs before sending or exchanging it to the cloud. This guarantees just the client approaches the information and not even the supplier. A Hierarchical Attribute Based Encryption technique has been proposed in [29] where fine grained get to control and furthermore elite is accomplished. A predicate encryption strategy is proposed in [30] utilizing different inquiry activities and protection of the clients is additionally guaranteed. This technique empowers the proprietors to control their own information and its lifetime.

Online Tech [31] has offered answers for give cloud security by encoding the information by strategies, for example, Full Disk Encryption which scrambles the information put away on a hard plate amid the booting activity and Whole Disk Encryption which scrambles the information very still utilizing the Advanced Encryption Standard calculation. A bit locker secret word is scrambled that guarantees that the information is protected if the gadget has been stolen. The Linux circle encryption is utilized to encode the information which exists in the bit. The primary preferred standpoint being that the apportioned information can be scrambled.

3. PROPOSED METHOD

The proposed method works initially when the cloud user wants to access the data from the data owner, he needs to get permission from the data owner. So, the proposed solution uses Elliptic Curve Diffie-Hellman method for adding a member in to the authorized list and also if any authorized person wants leave from the group it will handle.

From the authorized user all the users does not have the same permissions that is access roles, based on the user necessity theusers can have

- Read only
- Write
- Read and write
- Download

Authorized group members will get these kind of roles form the data owner by sending the requests.

Eliptic curve and Diffie-Hellman based computation mechanism for secure communication of cloud users and data owner.

Basic terminology

T= {E (Fp), n, e, f, C, p, mi, P_u ($K_{e)}$, P_R (K_i)}

E (Fp)**:** Elliptic curve equation

O: Order of the group

e, f: Curve coefficients

C: Group or cluster generator point (Cx, Cy)

P: Prime base point p ϵ E(Fp)

mi: i-th group member i ϵ [1,n]

P_u (K_e): Public keyof mi calculated through scalar multiplication operation

P_R (K_i): Private Secret key of mi, (a random integer)

Initially we are discussing with two party communication that is data owner and an cloud user how they compute their keys using elliptic curve dDiffie-Hellman.

Algorithm: Elliptic Curve Diffie– Hellman

Step 1: $O_e \leftarrow P_r(K_e)$ and $O_f \leftarrow P_r(K_f)$

Step 2: Calculate

$O_e \rightarrow P_u(K_e)$

$O_f \rightarrow P_u(K_f)$

$P_u(K_e) \leftarrow P_r(K_e) * C$

$P_u(K_f) \leftarrow P_u(K_f) * C$

Step 3: O_e sends $P_u(K_e)$ O_f

Step 4 :$O_f \rightarrow K_k(O_f)$ ⟶

$K_k(O_f) \leftarrow P_r(K_f) * P_u(K_e)$

Step 5 :O_f sends $P_u(K_f)$ O_e

Step 6 :$O_e \rightarrow K_k(O_e)$ ⟶

$K_k(O_e) \leftarrow P_r(K_e) * P_u(K_f)$

Step 7 :$K_k(O_{e,f}) \rightarrow K_k(O_e) = K_k(O_f)$ else got problem in computation.

The above algorithm creates secret key for two gathering interchanges. Give us a chance to expect dataowner Ne and Nf needs to convey safely through a mystery key. Right off the bat, Ne and Nf arbitrarily chooses private keys Pr (Ke), keys Pr (Kf) separately. Next, the two groups create open keys utilizing Pu(Ke) and Pu(Kf) gather generator point and trading their open keys into each other after that the two hubs compute secret keys Kk(Oe) and Kk(Of) independently lastly, both must produce square with comes about.

Algorithm: Joining of new user in to the group

Step 1: $O_c \leftarrow P_r(K_c)$

Step 2 :$O_c \rightarrow P_u(K_c)$

$P_u(K_c) \leftarrow P_r(K_c) * C$

Step 3 :O_{gm} sends $P_u(K_e)$, $P_u(K_f)$,$K_k(O_{e,f})$ O_c ⟶

Step 4 : Calculate

$O_c \rightarrow P_u(K_{c,e})P_u(K_{c,e}) \leftarrow P_r(K_c) * P_u(K_e)$

$O_c \rightarrow P_u(K_{c,f})P_u(K_{c,f}) \leftarrow P_r(K_c) * P_u(K_f)$

$O_c \rightarrow K_k(K_{e,f,c})K_k(O_{e,f,c}) \leftarrow P_r(K_c) * K_k(O_{e,f})$

Step 5 :O_c broadcasts intermediate key to O_e,O_f

O_c sends $P_u(K_{c,f})$ O_e

Step 6 : Calculate ⟶

$O_e \rightarrow K_k(O_{e,f,c})K_k(O_{e,f,c}) \leftarrow P_r(K_e) * P_r(K_c) * P_u(K_f)$

$O_f \rightarrow K_k(O_{e,f,c})K_k(O_{e,f,c}) \leftarrow P_r(K_f) * P_r(K_c) * P_u(K_e)$

The above calculation indicates joining of new client into the multicast group. Assume, if a client Oc needs to participate in a group. In the first place client needs sends join ask for message to information proprietor. Information proprietor will allow consent to new client Oc. client Oc chooses one private key Pr (Kc) and create open key Pu(Kc). Information proprietor sends all the moderate keys to new hub Oc. In the wake of accepting all the keys from information proprietor, Oc goes about as another group part and information proprietor again registers the all the new keys for group interchanges. At long last information proprietor communicate the keys into outstanding group individuals. Those perform calculations on got keys and produce another group key.

Algorithm: Joining of n new users into the group

Round i ∈ [0, n-2]

N_i G * (∏P_r(Nk)| k∈[0,i]^k≠i,j∈[0,i]), G * S_k(N_o.....) N_{i+1} ⟶

N_{n-1} G * S_k(N_o.....i-1 i+1.....n-1) N_i ⟶

The above algorithm represents a huge number of users wants join in a group so need to create all their keys and need to compute back the group key.

Algorithm: Leaving a user from the multicast group

Step 1 :$O_l$quit REQ O_{gm}

Step 2 :$O_{gm} \leftarrow$ new $P_r(K_{gm})$ ⟶

Step 3 : Calculates

$O_{gm} \rightarrow P_u(K_{gm})$

$P_u(K_{gm}) \leftarrow$ new $P_r(K_{gm}) * C$

Step 4 :O_{gm} broadcasts intermediate key values to all group nodes.

Step 5 : Nodes generates group key using their P_r.

The above calculation talks about how a client leaves from the group. Hub O1 need to leave from a group first client sends quit request for (QuitREQ) to information proprietor Ogm. Group manager concede consent and changes his private key. Next, Group administrator ascertains open key, moderate keys and communicate to all group members. Group individuals produce group key by utilizing their private keys.

Role based accessing algorithm:

From the authorized user all the users does not have the same permissions that is access roles, based on the user necessity that permissions are

- Read only
- Write
- Read and write
- Download

Authorized group members will get these kind of roles form the data owner by sending the requests.

Algorithm of role generation ()
User sends request to data owner
Request = user credentials + permission type
Data owner verifies the user credential
If(User==1)
{
Grant the permission
}
Else
{
Deny the permission
}

4. EXPERIMENTAL SETUP

In this segment we first present experimental results of the Encryption algorithm, secrecy preserving mechanism and group key management method. We then present an experimental comparison between the existing approach of CP-ABE, PGKM and proposed method of ECDH. The analyses were performed on a machine running UBUNTU 14.04 LTS with an Intel Corei3 CPU 2.50 GHz and 4 GB memory. Just a single CPU was utilized for calculation. Our model framework is executed in JAVA.

5. RESULTS AND DISCUSSIONS

This section present results and discussions about the adding a user to group, adding group of users to the group, removing a user from the group and authenticating a user and giving access permissions to the user.

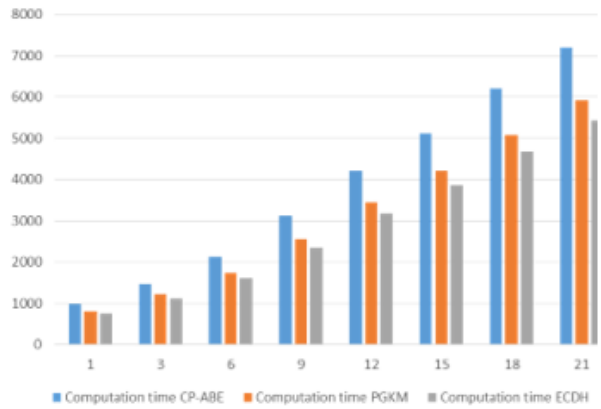

Figure 2. Time for adding one by one user to the group

Figure-2 shows the computation time for adding a single user or one by one user to the existing group that is group size varying from one member to twenty one members and here we compare three such mechanisms those are CP-ABE, PGKM and proposed mechanism ECDH. Figure-2 shows proposed method gives the good computation time than all other existing works.

Figure-3 shows the computation time for adding a group of users at the same time to the existing group and group size varying from one member to twenty one members and here we compare three such mechanisms those are CP-ABE, PGKM and proposed mechanism ECDH. Figure-3 shows proposed method gives the good computation time than all other existing works.

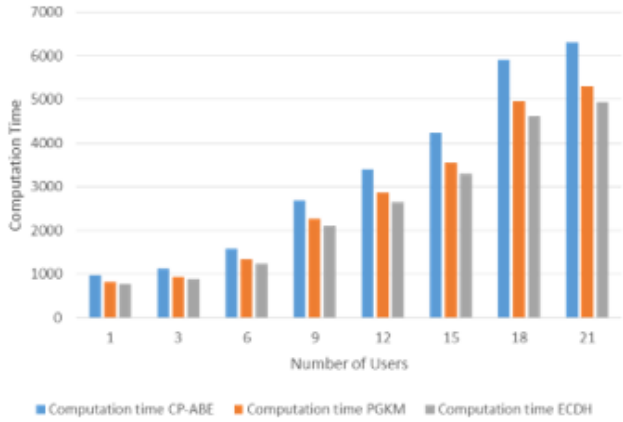

Figure 3. Computation time for adding a group of users at a time

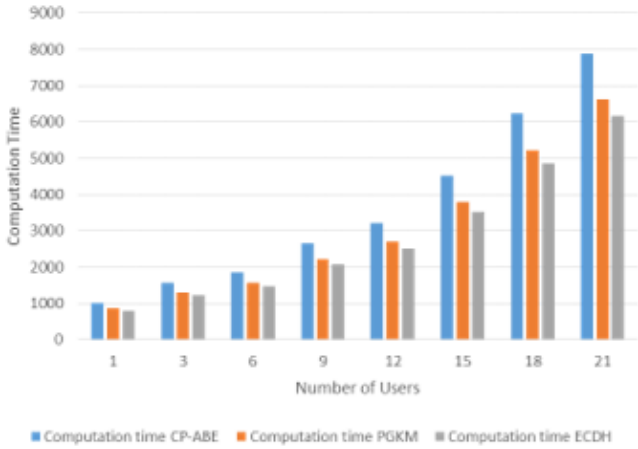

Figure 4. Time for removinga user from Grop

Figure-4 shows the computation time for removing a user from the group of users belongs to existing group that is group size varying from one member to twenty one members and here we compare three such mechanisms those are CP-ABE, PGKM and proposed mechanism ECDH. Figure-4 shows proposed method gives the good computation time than all other existing works.

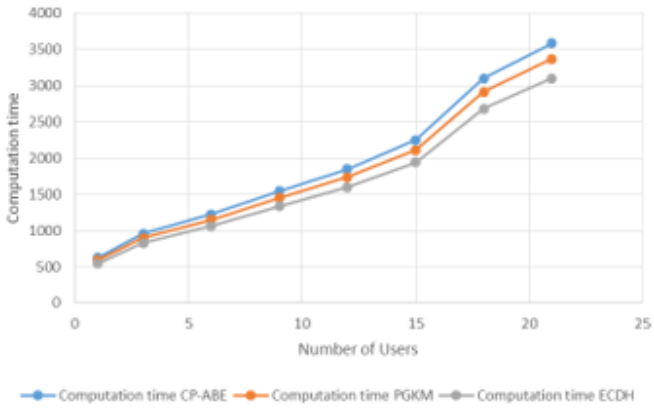

Figure 5. Computation time for users authorization

Figure-5 shows the computation time for authorization of user and giving the access privileges to the user. We compare three such mechanisms those are CP-ABE, PGKM and proposed mechanism ECDH. Figure-5 shows proposed method gives the good computation time than other existing works.

6. CONCLUSION

The proposed method works initially when the cloud user wants access the data from the data owner. He needs to get permission from the data owner. The proposed solution uses Elliptic Curve Diffie-Hellman method for adding a member into the authorized list and also if any authorized person wants leave from the group it will handle. The results show that the proposed method is better in handling group of users than other two mechanisms like CP-ABE and PGKM.

REFERENCES

[1] Institute FR. (2010). Personal Data in the Cloud: A Global Survey of Consumer Attitudes.

[2] From Hype to Future: KPMG's 2010 Cloud Computing Survey. http:// www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/, accessed in 2010.

[3] Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, et al.(2010). A view of cloud computing. Commun. ACM 53(4): 50–58.

[4] Global Survey: Has Cloud Computing Matured. http://www.avanade.com/Documents/Research%20and %20Insights/, accessed in 2011.

[5] Delerablée C. (2007). Identity-based broadcast encryption with constant size ciphertexts and private keys. In ASIACRYPT Lecture Notes in Computer Science 4833: 200–215.

[6] Zhou L, Varadharajan V, Hitchens M. (2011). Enforcing role-based access control for secure data storage in the cloud. Comput. J. 54(13): 1675–1687.

[7] Zhu Y, Hu H, Ahn GJ, Wang H, Wang SB. (2011). Provably secure role-based encryption with revocation mechanism. J. Comput. Sci. Technol. 26(4): 697–710.

[8] Akl SG, Taylor PD. (1983). Cryptographic solution to a problem of access control in a hierarchy. ACM Trans. Comput. Syst. 1(3): 239–248.

[9] Atallah MJ, Frikken KB, Blanton M. (2005). Dynamic and efficient key management for access hierarchies. In Proc. ACM Conf. Comput. Commun. Sec. 190–202.

[10] Hassen HR, Bouabdallah A, Bettahar H, Challal Y. (2007). Key management for content access control in a hierarchy. Comput. Netw. 51(11): 3197–3219.

[11] Di Vimercati SDC, Foresti S, Jajodia S, Paraboschi S, Samarati P. (2007). Over-encryption: Management of access control evolution on outsourced data. In Proc. VLDB 123–134.

[12] Blundo C, Cimato S, Di Vimercati SDC, Santis AD, Foresti S, Paraboschi S, et al. (2009). Efficient key management for enforcing access control in outsourced scenarios. In SEC (IFIP) 297: 364–375.

[13] Samarati P, Di Vimercati SDC. (2010). Data protection in outsourcing scenarios: Issues and directions. In Proc. ASIACCS 1–14.

[14] Gentry C, Silverberg A. (2002). Hierarchical ID-based cryptography. In ASIACRYPT (Lecture Notes in Computer Science) 2501: 548–566.

[15] Boneh D, Boyen X, Goh EJ. (2005). Hierarchical identity based encryption with constant size ciphertext. In EUROCRYPT Lecture Notes in Computer Science 3494: 440–456.

[16] Goyal V, Pandey O, Sahai A, Waters B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In Proc. ACM Conf. Comput. Commun, 89–98.

[17] Sahai A, Waters B. (2005). Fuzzy identity-based encryption. In Proc. EUROCRYPT, 457–473.

[18] Yu S, Wang C, Ren K, Lou W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In Proc. IEEE INFOCOM, 534–542.

[19] Zhu Y, Ma D, Hu C, Huang D. (2013). How to use attribute-based encryption to implement role-based access control in the cloud. In Proc. Int. Workshop Sec. Cloud Comput., 33–40.

[20] Goh EJ, Shacham H, Modadugu N, Boneh D. (2003). SiRiUS: Securing remote untrusted storage. In Proc. NDSS, 1–15.

[21] Ateniese G, Fu K, Green M, Hohenberger S. (2005). Improved proxy re-encryption schemes with applications to secure distributed storage. In Proc. NDSS, 29–43.

[22] Shamir A. (1984). Identity-based cryptosystems and signature schemes. In CRYPTO (Lecture Notes in Computer Science) 196: 47–53.

[23] Barreto PSLM, Libert B, McCullagh N, Quisquater JJ. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. in ASIACRYPT (Lecture Notes in Computer Science) 3788: 515–532.

[24] Boneh D, Crescenzo GD, Ostrovsky R, Persiano G. (2004). Public key encryption with keyword search. In EUROCRYPT (Lecture Notes in Computer Science) 3027: 506–522.

[25] Golle P, Staddon J, Waters BR. (2004). Secure conjunctive keyword search over encrypted data. In ACNS (Lecture Notes in Computer Science) 3089: 31–45.

[26] Boneh D, Waters B. (2007). Conjunctive, subset, and range queries on encrypted data. In TCC (Lecture Notes in Computer Science) 4392: 535–554.

[27] JAX-WS Reference Implementation. http://jax-ws.java.net/, accessed in 2013.

[28] HyperSQL Database. http://hsqldb.org/.

[29] Silverman JH. (2009). The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics), 2nd ed. New York, NY, USA.

[30] Miyaji A, Nakabayashi M, Takano S. (2001). New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundam. E84-A(5): 1234–1243.

[31] Barker E, Barker W, Burr W, Polk W, Smid M. (2011). Recommendation for key management—Part 1: General (revision 3). NIST, Gaithersburg, MD, USA, Tech. Rep. SP800-57.

[32] Jenkins RJ. (1996). ISAAC. In FSE (Lecture Notes in Computer Science) 1039: 41–49.

[33] SOAP Message Transmission Optimization Mechanism. http://www.w3.org/TR/soap12-mtom/, accessed in 2005.

[34] Pudovkina M. (2001). A known plaintext attack on the ISAAC keystream generator. Dept. Cryptol. Discrete

Math., Moscow Eng. Phys. Inst., Moscow, Russia, Tech. Rep. 2001/049.
[35] Aumasson JP. (2006). On the pseudo-random generator ISAAC. FHNW, Windisch, Switzerland, Tech. Rep. 2006/438.
[36] Caro AD, Iovino V. (2011). Java Pairing Based Cryptography Library. http://libeccio.dia.unisa.it/projects/jpbc/, accessed in 2011.
[37] Lynn B. (2007). Pairing-Based Cryptography Library. http://crypto.stanford.edu/pbc/
[38] Bouncy Castle Cryptography Library. http://www.bouncycastle.org/, accessed in 2013.
[39] Canetti R, Halevi S, Katz J. (2004). Chosen-ciphertext security from identity-based encryption. In EUROCRYPT (Lecture Notes in Computer Science) 3027: 207–222.
[40] Boneh D, Katz J. (2005). Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In CT-RSA (Lecture Notes in Computer Science) 3376: 87–103.
[41] Mell P, Grance T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 1-3.
[42] A. Merrihew, Cloud Computing: How to explain it to others in your organization [DB/OL].
[43] B. Butler, "Are Community Cloud Services the Next Hot Thing", [DB/OL].
[44] Samuels M. Community Clouds: Why they're a step too far for Organisations. [DB/OL].
[45] Linthicum D. SaaS is Cloud Computing's quiet killer app [DB/OL].
[46] Chriss A. Intuit Customer Solution Case Study [DB/OL].
[47]http://www.salesforce.com/assets/pdf/misc/WP_Forcedotcom-Security.pdf (2010-07-06)
[48] Juengs D. What is Platform as a Service [DB/OL].
[49]file:///C:/Users/staff/Downloads/CloudSecurityConsiderations_MicrosoftOffice365.pdf (2011-07-06)
[50] https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf (2012).
[51] Todorov D, Ozkan Y. (2013). http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf.
[52] http://www.questsys.com/cloudServices.aspx (2013-11-04)
[53]http://www.gemalto.com/press/Gartner_Magic_Quadrant_2013.html (2013-03-05)
[54]http://www.terremark.com/uploads/documents/WP14970.a.Online_Identity_Mgmt_03_PrePress.pdf (2012-10-23)
[55] Baize E. Cloud and Virtualization: Surpassing Current levels of security [DB/OL].
[56] http://www.druva.com/documents/Druva-inSync-Security-Q115-R54-10062.pdf (2014)
[57] Barr J, Narin A, Varia J. (2011). Building Fault-Tolerant Applications on AWS. Amazon Web Services, 1-15.
[58] Khalid U, Ghafoor A, Irum M, Awais Shibli M. (2013). Cloud Based Secure and Privacy Enhanced Authentication and Authorization Protocol. Procedia 22: 680-688.
[59] Zissis D, Lekkas D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems 28(3): 583-592.
[60] Acar T, Belenkiy M, Kupcu A. (2013). Single Password Authentication. Computer Networks 57(13): 2597-2614.
[61] Oracle, Private Database Cloud [DB/OL].
[62] Bernabe JB, Marin Perez JM, Alcaraz Calero JM, Garcia Clemente FJ, Perez GM. (2014). Semantic- Aware – multitenancy-authorization system for cloud architectures. Future Generation Computer Systems, (2014) 32: 154-167.
[63] Chadwick DW, Fatema K. (2012). A privacy preserving authorization system for the Cloud. Journal of Computer and System Sciences 78(5): 1359-1373.
[64] Saldhana A, Marian R, Barbir A, Jabbar SA. OASIS Cloud Authorization (CloudAuthZ) TC [DB/OL].
[65] http://www.vmware.com/files/pdf/partners/vmware-public-cloud-security-wp.pdf?src=vcld-2012-1-blog-PCSA%20whitepaper-ex-41 (2012)
[66] http://www.dell.com/learn/us/en/04/campaigns/dell-data-protection-solutions, (2013-11-06)
[67] http://www.wuala.com/en/learn/technology, (2014-01-03)
[68] Wang G, Liu Q, Wu J, Guo M. (2011). Hierarchical attribute based encryption and scalable user revocation for sharing data in cloud servers. Computers and Security 30(5): 320-331.
[69] Fan CI, Huang SY. (2013). Controllable privacy preserving search based on symmetric predicate encryption in cloud storage. Future Generation Computer Systems 29(7): 1716-1724.
[70] http://www.onlinetech.com/cloud-computing-hosting/overview (2014)
[71] Popa L, Yu M, Ko SY, Ratnasamy S, Stoica I. (2010). Cloud Police: taking access control out of the Network. ACM Sigcomm Workshop.