JNNCE Journal of Engineering & Management – A Peer Reviewed Bi-annual Journal
Available online @ https://jjem.jnnce.ac.in
ISSN: 2582-0079 (O)
https:// www.doi.org/10.37312/JJEM.2019.030202
Indexed in International Scientific Indexing (ISI)
Impact Factor Value: 1.025 for 2018-19
Volume: 3, Issue: 2
July - December 2019
Date of Publication: 12-30-2019

Comparative Analysis of Key Management Methods for Online Data Sharing in Cloud

Mohan Naik R
Asst.Professor, Dept of ECE
SDMIT,UJIRE – 574240
m.naik5785@gmail.com

Dr. S.V.Sathyanarayana
Professor, Dept of ECE,
JNNCE, Shimoga-577201
svs@jnnce.ac.in

Abstract

Data sharing in cloud computing facilitates various components to uninhibitedly distribute the group data information, that which improves the intensity of effort in supportive conditions and has transversely the originate into ensuing appliances. Conversely, an approach to make sure the precautions of data sharing inside and the best approach to with effectiveness share the re-corrected wisdom in an extremely grouping method square determine substantial difficulties. A key management policy is effectually employed for the purpose of generating a distinctive convention key for ample members to promise the security of their prospect communications, and this agreement can be allied in cloud computing for the purpose of assisting protected and skilled data distribution. At this point, an original square structure dependent key management that upkeeps diverse associates, which possibly will adjustable expand the quantity of associates and besides supported the organized group data sharing model, with the intention of diminishing the calculation multifaceted nature completely.

Key words: Key Management, cloud computing, group data sharing.

I. Introduction

Cloud computing and cloud storage has bowed out to be passionately deliberates concerns in late decades. Every area unit dynamical the method we tend to live and greatly improve. At this time, in consequence of limited stock property and additionally the concentration for profitable admission, on the whole amass each sort of data in cloud servers, that is furthermore an improved than average decision for firms and linking to endure from the overhead of assigning and sustaining instrumentation once data information zone unit hang on in the neighborhood. The cloud server provides partner open and beneficial amassing stage for individuals and associations, at any rate it additionally presents security concerns.

A cloud framework is likewise exposed to assaults from each malevolent clients and cloud sup-pincers. In these situations, it is critical to assurance the safeguard of the deposited data information. Few plans were proposed to safeguard the security of the redistributed information. The above plans just considered security issues of a solitary information proprietor.

Anyway in certain applications different information proprietors might want to safely share their information in a group method.

Along these lines, a convention that maintains protected group information distributing underneath cloud computing is required.

A key understanding convention is utilized to create a typical convention key for numerous members to guarantee the security of their later communications [1], and this convention can be connected in cloud computing to help protected and effective data sharing. Since it was presented by Diffie-Hellman in their original paper, the key concord proto-col has turned out to be one of the major cryptographic natives The essential adaptation of the Diffie Hellman convention gives an effective answer for the issue of making a typical secret key between two members. In this paper, apply key management techniques to different cloud situations More explicitly our commitments are

Distinguishing key management strategies for cloud data storage. Looking at among key management techniques.

1,.Applying key management strategies to different cloud conditions.

2. Recognize applications and reasonable strategies that can be connected. Elliptic curve based Key management.

3. Comparing symmetric key algorithms with Asymmetric key algorithm.

4. Discussing experimental results that adopted in key management.

The manuscript is composed as pursues. In segment II, depicts related work in the different key management approaches for the purpose of cloud data storing. Segment III depicts key management strategies in cloud Section IV Section presents correlations among the key management techniques. Segment V presents key management techniques for different scenarios. Segment VI presents appliances that can develop key management approaches. Segment VII presents applying key management schemes for a number of settings. Section VIII presents Elliptic curve based key management. section IX presents Experiment results and comparison. section X Conclusion.

II. Related WORK

Cloud Key Management (CKM) framework comprises of Cloud Key Management Customer (CKMC) and Cloud Key Management Server (CKMS)[2]. CKMC presents a service for three major cloud administration models, together with Software, proposal or Infrastructure (as a Service). CKMS cooperates with CKMC utilizing CKM interoperability convention, which interfaces with Symmetric Key Management System (SKMS) and Public Key Infrastructure (PKI) utilizing symmetric key management proto-col and uneven key management convention separately, as appeared in Figure 1.

The Cloud Key Management Interoperability Protocol (CKMIP) sets up a solitary complete convention for the purpose of communication connecting CKM servers and cryptographic consumers [2]. By means of characterizing a convention that is possible to be employed by any number of clouds.

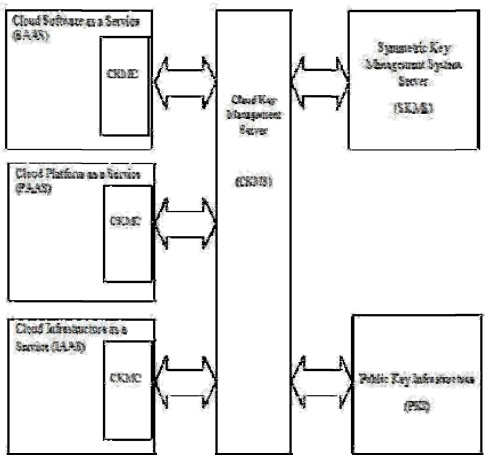

Figure 1: Cloud Key Management Infrastructure

Cryptographic customer, extending from multi-inhabitant execution, it promotion dresses the basic requirement for a far reaching key management convention. It is worked in the cloud computing framework, possibly can send compelling bound together key management for the entirely encryption, endorsement based gadget validation, advanced signature and supplementary cryptographic capacities. during seller backing of CKMIP, a cloud computing sys-tem will almost certainly solidify key management in a solitary endeavor key management framework. It lessens operative and framework expenses despite the fact fortifying prepared controls and administration of safety strategy.

Ivan Damgrd et al [3]: The creator has thought about that the applications including various servers in the cloud that experience a succession of online stages in which the servers impart, isolated by disconnected stages in which the servers are inactive. All through the disconnected periods, servers need to safely store touchy data, for example, cryptographic keys. Appliance like this incorporates numerous situations where protected combined calculation is redistributed to the cloud, and specifically various online closeouts and benchmark calculations with private sources of inputs. Creator indicates that the proto-col coming about because of the above talk as the CKM convention, or presently PCKM.

Dr. Atulbhai Patel et al [1]: The paper portrays cloud computing security by means of utilizing the key management includes every one of the subtleties of the procedure to deal with keys cautiously adequate to guarantee mystery. The federated personality the executives and Hierarchical Identity Based Cryptography (HIBC) delineates in what manner can the framework produces and convey general society and private keys to customers and servers. Contrasted and the present Ws-Security advance, the expert presented move toward in this document has favorable circumstances in streamlining public key dispersion and lessening [SOAP] description estimate.

Ching-Nung Yang et al[4]: In the recommended plan, the main security concern of cloud computing is predominantly the cloud supplier necessity guarantee that their foundation is protect, and that avoid unlawful information gets to from outcasts, different customers, or still the unapproved cloud representatives. In this document the creator depicts cloud security maintenance together with key understanding and validation utilizing Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial dependent mystery sharing.

Wei Zhang et al[5]:Here the creator characterizes and tackle the difficult issue of protection saving multi-keyword ranked search over encrypted cloud information (MRSE). Author set up a lot of severe safety fundamentals for this kind of a protected cloud information use construction.

In the middle of different multi keyword semantics. Trials on this current authenticity dataset extra demonstrate anticipated plots to be sure present low overhead on computation and communication. XiaoChun Yin et al [6]: PKI-dependent cryptography for the purpose of secure cloud data storage with the assistance of ECC. In this paper the creator concentrate on the security concerns of accumulates confidential and delicate data information in the cloud storage administration.

Piotr K.Tysowski et al[7]: Novel alterations to trait dependent encryption are formulated for the purpose of permit acceptable customers access to cloud data dependent on the implementation of required qualities with the end goal that the advanced computational load from cryptographic responsibilities is allotted to the cloud supplier and the all-out communication cost is brought down for the mobile customers. In addition, data information re-encryption might be on the other hand achieved by the cloud supplier to diminish the price of customer repudiation in a mobile customer condition whereas saving the security of customer information put away in the cloud.

Shilpi Singh et al [8]: The shortcoming in clients validation procedure and absence of

compelling security strategy in cloud storage prompts numerous difficulties in cloud computing. This document introduces a plan that not just gives defense of client's confidential information of accumulating and getting to more than the cloud yet additionally confirmation of the client to the cloud server utilizing ECC.

Sikhar Patranabis et al [9]: Demonstrates the Data information proprietors would in a perfect world need to accumulate their information/records online in an encrypted style, and entrust decryption authentications for a portion of these to clients, although holding the ability to deny entrance anytime of time. A valuable arrangement in such manner possibly be one that facilitates clients to decrypt various classes of information utilizing a solitary key of consistent magnitude that could be proficiently communicated to different consumers. Creator likewise arrange uncommon spotlight on how the independent KAC plan can be proficiently joined with communicated encryption to take into account m data information clients and m0 data information proprietors while decreasing the lessening the safe channel prerequisites.

Fuchun Guo et al[10]: Identity-based encryption (IBE): Procedure for decrypting numerous ciphertexts utilizing a solitary decryption. An IBE framework includes a confided in private key generator that grasps an ace mystery key and concerns a mystery key to each customer dependent on the customer character. Every client gets a communication that has been effectively encrypted utilizing her particular id and certain public limitations, and possibly decrypt a similar utilizing the mystery key dispensed to her by the confided in party. Reduced key IBEs have been anticipated in this article.

Pandi Vijayakumar [11]: Key Management for cloud data storage: at this time paper currents reasonable key management strategy in accordance with cloud condition. It characterizes the location to amass the keys for explicit key management strategy. It additionally depicts highlight of every methodology when concern appropriate key management strategy.

The above writing clarified all the related key management techniques that are necessary in the cloud condition and furthermore depicts which cryptography strategy (symmetric or asymmetric key) requirements to connected to explicit cloud condition, highlight of each methodology, where the keys should be put away. What pursues are clarifying all the related key management in cloud dependent on the applications and highlights.

III. Key management methods in Cloud

Key is significant viewpoint for looking after protection. e.g keeping up security of household, keeping up security of information [11]. Cryptography key can be utilized for the purpose of maintaining the information private starting the others. Hence, when there are different customers in the structural arrangement, Key Management System (KMS) require to make the key for each customer, distribute it to the customers. In the scenario where the event that the key is smashed, KMS wants to recoup the key. During the occurrence that key isn't being employed, KMS wants to wipe away the key. Key is associated with the metadata. Metadata enclosed data about key label, key identifier, Key life cycle stages, cryptographic scheme, and limitations for the key, length of key, key use tally.

Key life cycle include different stages, for example, formation, instatement, complete dissemination, active, inert and end [12]. Key administration is the set of strategies includes generation, dispersion, stockpiling, repudiating, confirming keys. It is possible to apply key management to cloud infrastructure. The accompanying segment depicts different key managements dependent on the prerequisites.

3.1 Management of Key at Client Side

Here, information will be put away at cloud specialist supplier side in encrypted structure. Customer might be slender for example cell phone. At this point, keys will be kept up at client side. Normally this methodology is taken in Homomorphism.

3.2 Key management at Cloud Service Provider Side

Here, keys are kept up at cloud specialist supplier side. On the off chance that the key is lost, client is unfit to peruse information that is available at cloud. Information is put away in the encrypted structure and decrypted by the way to acquire it in the unique structure.

3.3 Management of Key at client and CSP Sides

Here, key is separated into two different sections. One section is put away at client side and remaining portion is put away at cloud side. On the off chance that the two sections are joined together, it is conceivable to recover the information appropriately. Therefore information remains the safe and can be constrained by the client. Whole key at Cloud side. In the event that piece of the key is lost, information can't be well again.

3.4 Key Splitting Technique

Along these lines arrangement is additionally versatile. Cloud specialist suppliers and client don't have to keep up Content supplier share information in cloud in order to available by different clients. Key is splitted and conveyed among the clients. In the event that specific client desires to acquire to the information available from the cloud, first he/she wants to get the incomplete keys from the clients.

In the event that k out of n keys is joined, at that point client can encrypt and decrypt the data information.

3.5 Key Management at Centralized Server

This methodology utilizes asymmetric key methodology. Information is encrypted together with the public key pack away in key server. The data information at cloud side is put away in the encrypted structure. The client gets to the data information. It is effectively decrypted by private key kept up at every client.

Inconvenience of this technique is that when the key server is slammed, its single purpose of disappointment [2, 12, 13]. Each client produces public and private keys. Public keys are put away at key server. Assume mobile client needs to impart data information to home/desktop client. They need to encrypt the information together with public key of desktop client. In this manner desktop client will get to information with its private key.

3.6 Group Key Management for Cloud Data Storage

Information is contributed in cloud with confided in individuals from the cluster. Group key is set up for the purpose of verifying information at cloud side. Group key is created by the fractional keys kept up at every client. In the event that specific group individuals need to get to the information, group key applied to get to the data information. On the off chance that part moves away from the group, and then its group key is created once more. On the off chance that part links the group, and then its group key is set up along with individuals [12, 13, 14].

IV.COMPARATIVE CHART OF KEY MANAGEMENT METHODS

At customer side, the key is kept up at customer side. Accordingly, it is observed to be adaptable, protected.

At Cloud specialist organization side, public keys of clients are put away at Cloud. Here, the cloud is versatile geographically; however this strategy is extremely no safe as for customer. This is supposing that public key is snatched, along these lines customer is unfit for the purpose of encrypting the information. For instance, the private key is kept up by every customer and public keys during the cloud side, this methodology utilizes asymmetric key methodology.

In case of overseeing key at client region and cloud specialist supplier side, splitted key is kept up at the two sides. Comprehensive key is created by means of consolidating splitted (incomplete) keys from the two sides. Customer utilizes this key for the purpose of encrypting and decrypting the information. Information is put away in encrypted structure in cloud. Consequently this methodology is versatile and

protected. This methodology is need in adaptation to internal failure in such a case that customer machine is fizzled, unfit to improve the key. This methodology utilizes symmetric key methodology.

In key part system, incomplete key is kept up at every customer. Key is shaped by consolidating k out of n fractional keys. At this point, this key is utilized for the purpose of encrypting and decrypting the information. This strategy is considered as versatile and protected. Incomplete key is kept up through every customer. It is considered to be adaptation to non-critical failure. Regardless of whether some halfway keys are missing, key is created by removing k from n keys. Here, this methodology utilizes symmetric key methodology.

During the process at Centralized Sever, public key of every customer is put away at focal server. It is to be noted that private key is with every customer. Such as, clients are expanding to utilize cloud administration, this methodology is observed to be no adaptable, protected and adaptation to internal failure. Unified methodology causes single purpose of disappointment. This methodology utilizes asymmetric key methodology. From Table I. it is seen that key part procedure is appropriate in light of the fact that it fulfills properties, for example, adaptability, security, and adaptation to non-critical failure.

V.KEY MANAGEMENT METHODS FOR VARIOUS SCENARIOS

In this segment, depicting different situations, for example, locally established methodology, redistributed private cloud, nearby network cloud, re-appropriated network cloud, public cloud and hybrid cloud situation. Security Check Post (SCP) is given to ensure the genuineness of client. At this point, the appropriate key management strategy is effectively employed so as to verify client data information stockpiling [16, 17, 18].

In this area, portraying different situations, for example, locally established methodology, redistributed private cloud, nearby network cloud, re-appropriated network cloud, public cloud and hybrid cloud situation. SCP is given to ensure the credibility of client. In this scenario, reasonable key management strategy is effectively employed so as to verify client information stockpiling [16,17,18].

5.1 Home based Cloud Scenario

Fig.2 depicts Home based cloud situation. Clients U1, U2 are in a similar group. These clients might utilize key part appliances. It utilizes causative group key agreement. Customers U4, U5, U6 are not in a similar group. Every client utilizes symmetric key methodology and keeps up isolated key. Their keys are put away at Key server. In case of non-locally established client, permits of the entrance asset depend on the ID of client. Such client can utilize asymmetric key methodology. e.g User U7,U8 and U9 are non-home based client. These clients accumulate private and public key in possess gadget. SCP limits permit of asset for these clients.

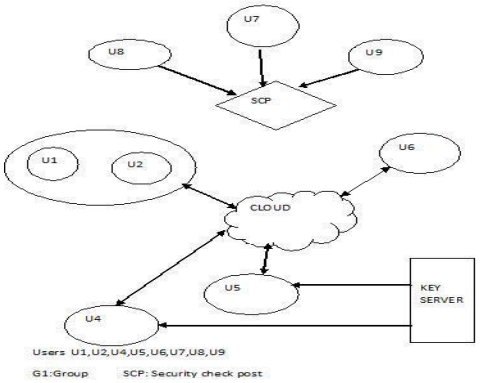

Figure 2: Home based Cloud

SCP regulates the entrance of cloud asset from clients. Clients U1, U2 are in a similar cluster. They utilize key dividing scheme. Every client in the group encryptsodes information next to own, transfer it to the cloud. Key will created subsequent to consolidating fractional key from k clients out of n users. Customers U4, U5, U6 are not in a similar cluster. These clients utilize asymmetric cryptography scheme. These clients

effectively encrypt the information through public key and store/transfer the information at cloud server. Information will be effectively decrypted through client private key. It might be put away at client cell phone. Public keys are put away at key server.

5.3 Onsite Community Cloud

Every community association will send its very own cloud stage. Clients in the organization don't actualize any key management strategy. Be that as it may, clients that is element of other association utilize symmetric key way to deal with permits the asset from other com-munity association. Every client key will be put away at community associations key server. SCP is given to get to the asset from the association cloud. While considering the Fig.4 there are four associations to be specific association C, I, E and A. Associations C and I have their individual cloud stage. Association E and I gets to the administrations through SCP.

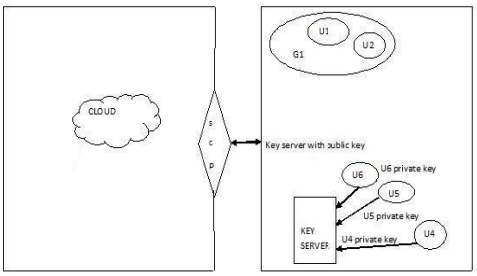

Fig3.Outsourced Private Cloud Scenario

5.4 Outsourced Community Cloud Scenario

Here, association gets permission of asset from re-appropriated cloud. Clients in the community association utilize asymmetric cryptography advances. Information will be effectively encrypted through public key of every client and decrypt through the private key of client. Public keys will be put away in association key server.

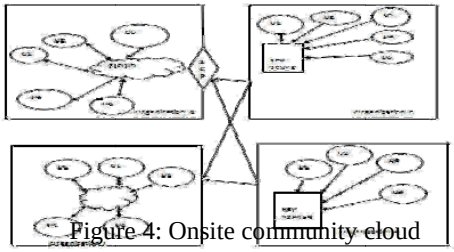

Figure 4: Onsite community cloud

5.5 Public cloud scenario

In this methodology, clients in a similar group utilize key splitting scheme. Clients not in the cluster utilize symmetric cryptography scheme. Information is effectively encrypted and transferred to Cloud server. Client takes the information from cloud server and effectively decrypts next to them. Fig. 6 depicts U1, U2 are in a similar group. They purposefully make use of key splitting scheme at the clients U4, U5, U6 and U7 utilizes symmetric key methodology.

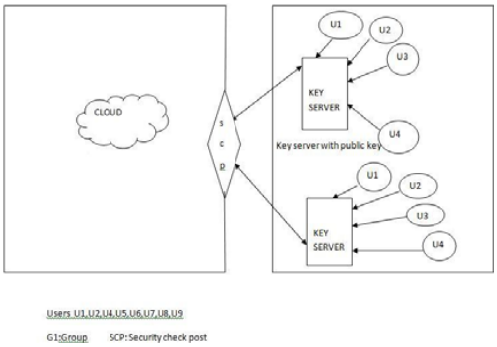

Figure 5: Outsourced community cloud

VI.APPLICATIONS THAT CAN USE KEY MANAGE-MENT METHODS IN CLOUD

Distinguishing the application classes is dependent on the way of communication, stockpiling and preparing of information dependent on cloud. Subsequent table II depicts application classes, applications and the procedure of key management strategies are reasonable for specific application class.

For Audio/Video conferencing, every part keeps up incomplete key and communication is conceivable subsequent to creating group key. In case of this application class, either key splitting

strategy or group key management technique ought to be utilized. For broadcasting, client ought to sustain key to confirm and approval to cloud server. During the scenario of collective server class application, every server keeps up fractional key and computation/communication

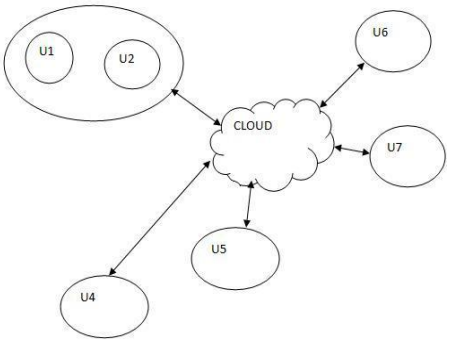

Figure 6: Public cloud scenario

VII. KEY MANAGEMENT AT VARIOUS SCENARIOS

Table III shows different cloud conditions [11]. It occurs reasonable key management strategy based on cloud condition. It characterizes the location to accumulate the keys for explicit key management strategy. It additionally depicts highlight of each methodology during the case if concern appropriate key management strategy. It likewise portrays the kind of cryptography strategy (symmetric or asymmetric key) wants to connected to explicit cloud condition, highlight of each methodology, where the keys should be stored.

VIII. ELLIPTIC CURVE CRYPTOGRAPHY BASED KEY MANAGEMENT

What pursues are the subtleties of ECC and Ellipic Curve Diffie Hellman Key Exchange Algorithm [19]. A significant number of the principles utilizes public key cryptosystem for verification reason. RSA is one among them. If there should be an occurrence of RSA encryption plan, as security builds the key length additionally expands which prompts high preparing in the clouds. Elliptic Curve Systems which are connected in numerous Cryptographic applications were presented in 1985 is possible subsequent to creating a group key. In case of substance sharing, either key management at cloud or key management at server approach ought to be utilized. This relies upon the specific application.

independently by Neal Koblitz and Victor mill operator [20].

ECC is one of the difficult frameworks created to furnish elevated security with littler key size. ECC is institutionalized through IEEE and announced in IEEE P1363 std.

Elliptic Curves are simple capacities which can be plotted as smooth circling lines in (x,y) plane. Taking everything into account, cubic equation for Elliptic Curve can be given by utilizing Generalized Weierstrass equation as given in Equation (1)

In which a_1; a_2; a_3; a_4; a_5; a_6 2 F_p and p represents a prime number. Condition 1 of Elliptic Curve over F_q is a lot of arrangements (x; y) 2 F_p together with extraordinary point o, known as point at infinity. On the off chance that normal for field is not one or the other '2' nor '3' at that point Equation 1 can be composed as

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

$$E : y^2 = x^3 + Ax + B \quad (2)$$

In majority of places, Equation 2 is utilized for some applications, with discriminant condition provided by Equation

$$4a^3 + 27b^2 \# 0 \quad (3)$$

Elliptic Curves over major field are effectively employed for carrying out Secret Sharing. 8.1 Elliptic Curves over GF(P)

An elliptic curve characterized over major field Z_P is acquired through choosing the factors a and b from the field Z_P. This curve includes the complete focuses (x,y) which accomplish the elliptic curve condition modulo p (in which x and y are has a place with Z_P). Elliptic curve over major field is provided by Equation (4)

Expansion and increase technique in an elliptic curve group over major field is provided as pursues. Give the focuses a chance to be P = (x_1; y_1) and Q = (x_2; y_2) in the elliptic group E_p(a; b) and O indicate the point at infinity.

The increase kP is gotten by rehashing the elliptic curve expansion task k times by a similar expansion equation. The scalar point augmentation over A can be characterized as kP = P + P +.... +P (k times). In the event that P; Q 2 A, the expansion P + Q represents a point R.

The line going throughout P and Q captures the bend at a point known as R. The impression of - R will be R as for the x-axis [29]. This is referred to as point expansion as appeared in Figure 9.

In the event that two cover for example P = Q, at that point R= P + P, it turns into a digression at P, that converges the curve at - 2P, The picture of - 2P on the transformed indication of y position is the subsequent effect of expansion of P+P which situated on the bend E/FP. It is referred to as point serving as provided in figure 8. The abnormal state of trouble of understanding the Elliptic Curve Discrete Logarithm Problem (ECDLP) gives the security superiority of the ECC. ECDLP indicates that, in case of an elliptic curve E over a prime limited field FP, the focuses P; Q (FP) and P is of request n, discover the whole number k 2 [0; n 1] with the end goal that Q = kP. The number k is regarded as the discrete logarithm of Q to the base P, signified as $k = \log_P Q$.

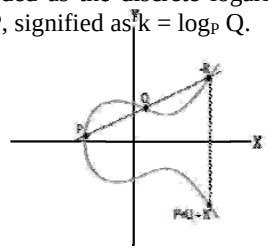

Figure 7: Point Addition

8.2 Elliptic Curve Encryption/Decryption

Assume client A needs to transmit a message P_m to client B subsequently client A haphazardly

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \quad (4)$$

picks a positive whole number k, private key d_A. The public key of is created as $P_A = d_A G$ and the figure content C_m is delivered with comprising of pair of focuses.

$C_m = (kG, P_m) + kP_B$

In which G indicates the base point selected on the elliptic curve, $P_B = d_B G$ represents the public key of B and d_B points out the private key of B. A will transmit the figure content C_m as encrypted message to B. in order to decrypt the figure content, B upsurges the primary point in the pair through its private key d_B and carries off the outcome from the second point in order to acquire the initial message P_m [13].

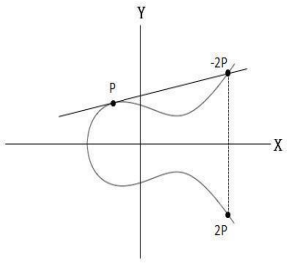

Figure 8: Point Douling

$P_m + kP_B - d_B (kG) = P_m + k (d_B G) - d_B(kG) = P_m$

8.3 Elliptic Curve Diffie-Hellman (ECDH) Key Exchange

In general, to encrypt/decrypt the bulk quantity of data Symmetric-key cryptosystems are used due to its faster computation than public-key cryptosystems. To create a secret key among two users for a single conference Elliptic Curve Diffie-Hellman key replace method on elliptic curve can be used which is explained beneath: assume that clients A and B intends to make sure the identical opinion regarding a secret key, which possibly be exploited for secret key cryptography. It is to be observed that, A will generate private key d_A and a public key $P_A = d_A G$, in which G indcites the originator of the elliptic curve. A transmits P_A to B. Fundamentally, B will generate private key d_B

and a public key $P_B = d_BG$. B transmits P_B to A. Once receiving the A's message, B generates d_B (P_A) = d_Ad_BG. Once receiving the B'ss message, A generates d_A (P_B) = d_Ad_B. At this point, both A and B can exploit d_Ad_BG, which indicates a point on the provided elliptic curve, as a typical mystery keys. The client first logins into the cloud and verify himself. After validation client utilizes two methods ECDH key trade and Symmetric key scheme for the purpose of encrypting and decrypting the data [8].

IX. Experimental Results

9.1 Assessment of essential key size for different algorithms dependent on identical dimension of security.

Here considering two execution measurements, for example, computation time and communication time. During the case of cloud condition when we implement symmetric key schemes, the qualities of cloud ought not to be disregarded. In this manner we led the investigation which thinks about symmetric key algorithms with asymmetric algorithm. The outcomes obtained from our anticipated plan are contrasted and the TGDH[21], BS[22], WU[23], Zhang[24], NTRU[25], EGKM[25] and RSAGKM[11] algorithm and contrasted and Elliptic curve Diffie Hellman Algorithm (ECDH). When contrasted ECDH and every single other capacity, the convolution item utilizes additional computation time and expansion utilizes less computation time. For estimating the computation time for different numerical activities, the tried and assessed structure is actualized in JAVA (Windows XP Operating System) for a collection of 1000 clients and the computation time for various key sizes with the current approaches to play out the rekeying task is associated. Even though RSA, ElGAMAL and Diffie Hellman are secure asymmetric key cryptosystem, their security accompanies a value their huge keys. For Elliptic Curve Cryptography execution subsequent thought should meet.

1. Appropriateness of strategies accessible for streamlining limited field number juggling like addition, squaring, multiplication, and reversal.

2. Appropriateness of strategies accessible for streamlining elliptic curve number juggling like point expansion, point multiplying, and scalar duplication.

3. Constraints of a specific computing condition e.g., speed, stockpiling, code measure, door tally, control utilization.

4. Constrictions of a specific correspondences condition e.g., data transmission, response time. Effectiveness of ECC is relies on components, for example, computational overheads, key size, data transfer capacity, ECC gives higher-quality perbit which integrate higher velocities, lower control utilization, transmission capacity investment funds, stockpiling efficiencies, and littler endorsements which is basic in distributed computing so as register quicker and with security.

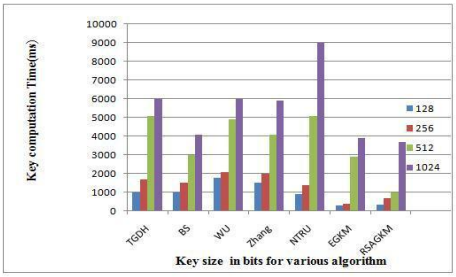

Figure 9: Key computation time for various algorithms

X.CONCLUSION

The ECDH algorithm centers for the most part around the minimization of computation complexity because of its key size and in each key refreshing time of a cloud user. However, when the key size increments as in RSAGKM (for example 1024 bits) the computation time additionally enlarging for the updation of a solo key from the dynamic multicast group. Based on the capacity multifaceted nature, the quantity of keys to be accumulated by the group individuals is marginally expanded if the key size expanded.

Table IV describes the various key size in bits of symmetric vs. asymmetric algorithm where EC scheme produces same security with reduced

key size and also reduces commutation and communication cost. The ECDH utilized so as to figure the group key along these lines keeping up the decreased communication intricacy for both the join and leave tasks in examination with other key management algorithm. By distinguishing appropriate key management approaches by utilizing it to different cloud situations and dissecting as for symmetric and asymmetric algorithm.

References

[1] Dr. Atulbhai Patel and Kalpit Soni, "Cloud Computing Security using Federated Key Management, International Journal Of Engineering And Computer Science, 2014, 3, 2, 3978-3981.

[2] Sun Lei and Dai Zishan, "Research on Key Management Infrastructure in Cloud Computing Environment", Ninth International Conference on Grid and Cloud Computing, 2010, 404-407, october, IEEE.

[3] Ivan Damgrd and Thomas P. Jakobsen, "Secure Key Management in the Cloud", 14th IMA International Conference on Cryptography and Coding, 2013,

[4] Ching-Nung Yang and Jia-Bin Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", International Symposium on Biomet-rics and Security Technologies, 2013,IEEE.

[5] Wei Zhang, Student and Yaping Lin and Jie Wu "Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing", IEEE TRANSACTIONS ON COMPUTERS VOL. 65, NO. 5, MAY 2016.

[6] XiaoChun Yin and ZengGuang Liu, "PKI-Based Cryptography for Secure Cloud Data Storage Using ECC", ICTC 2014, 194-199, May, IEEE.

[7] Piotr K.Tysowski and M.Anwarul Hasan, , "Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds IEEE TRANSACTIONS ON CLOUD COMPUTINGVOL.1,NO.2,JULY-DECEMBER 2013.

[8] Shilpi Singh and Vinod Kumar, "Secured Users Authentication and Private Data Storage-Access Scheme in Cloud Computing Using Elliptic Curve Cryptography", 2015,791-795,IEEE.

[9] Sikhar Patranabis and Yash Shrivastava and Debdeep Mukhopadhyay "Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on the Cloud", 2016,1-14,IEEE.

[10] Fuchun Guo and Yi Mu and Zhide Chen. "Identity-based encryption: how to decrypt multiple ciphertexts using a single decryption key" In Pairing-Based CryptographyPairing 2007, pages 392406. Springer, 2007.

[11]Pandi Vijayakumar and Ramu Naresh and Lazarus Jegatha Deborah and SK Hafizul Islam "An efficient group key agreement protocol for secure P2P com-munication"SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2016; 9:39523965 ,August 2016.

[12]Sandro Rafaeli, "Survey of key management for secure group communication", ACM Computing Surveys, Vol. 35, No 3, Sept 2003.

[13]Yacine Challal, "Group key management protocols: A novel taxonomy", IJIT Vol 2, No 1 2005.

[14]Kuei-Yi Chou, "An Efficient and Secure Group Key Management Scheme Sup-porting Frequent Key Updates on Pay-TV Systems", IEEE 11th International conference on Trust, 2012 Security and Privacy in Computing.

[15]Lee Badger and Tim Grance and Robert Patt Corner Jeff Voas, "Cloud Computing Synopsis and Recommendations" in NIST Special Publication 800-146 , May 2011.

[16]NIST," Cloud Computing Synopsis and Recommendations", Special publication 800-146, May 2012.

[17]Yung-Wei Kao and Kuan-Ying Huang and Hui-Zhen Gu and Shyan-Ming Yuan, "Cloud: a user-centric key management scheme for cloud data protection", IET Journal, 28 January, 2013.

[18]JV Aghav and CV Deshpande and AS Shetye and SS Ghuge, "Towards a Web-JDK: Extending openJDK 7 for client file system access over cloud" in Information Communication Technologies (ICT), 2013, 11 April 2013.

[19]Shalini I S, Mohan Naik R, and Dr.S V Sathyanarayana, "A Comparative Analysis of Secret Sharing Schemes with Special Reference to Group Communication Applications", IEEE International Conference on Emerging Research in Electronics and computer science and Technology (ICERECT-2015). December 2015.

[20]Koblitz, N, "Elliptic Curve Cryptosystem", Journal of mathematics computation, Vol. 48, No. 177, pp203- 209, 1987.

[21]Rahman, R. H. and Rahman M. L:"An efficient group key agreement protocol for ad-hoc networks": 5th International Conference on Electrical and Computer Engineering, ICECE 2008, 2022, (2008).

[22]Boneh D and Silverberg A. "Applications of multilinear forms to cryptography". Contemporary Mathematics 2003; 324:7190.

[23]Wu Q and Mu Y and Susilo W and Qin B and Domingo-Ferrer J. Asymmetric group key agreement in: EUROCRYPT 2009. In LNCS, Vol. 5479. 2009; 153170.

[24]Zhang L and Wu Q and Qin B and Domingo-Ferrer J.Identitybased authen-ticated asymmetric group key agreement protocol in: COCOON 2010. In LNCS, Vol. 6196. 2010; 510519.

Table I: APPLICATIONS CLASS, APPLICATION AND KEY MANAGEMENT METHOD

Key management Schemes	Scalability	Security	Fault tolerence	Cryptography Algorithm Suitable
At Customer side	Yes	Yes	No	Symmetric
At Cloud Service Provider side	Yes	No	No	Asymmetric
Overseeing key at client side and cloud specialist organization	Yes	Yes	No	Symmetric
Key splitting scheme	Yes	Yes	Yes	Symmetric
At Centrailized server	No	No	No	Asymmetric

Table II: DIFFERENT APPLICATIONS AND METHODS USED FOR KEY MANAGEMENT

Application Class	Applications	Methods required to apply
Conferencing	Audio, Video Conferencing	Key Splitting Method, Group Key management
Broadcast	Television broadcasting	At user side and at service provider side
Collaborative Server	Load balancing	Key splitting method, Group key management
Content Sharing	Dropbox, CloudMe, Google Drive, Skydrive	Key management at Cloud and at service provider side
Content Sharing	Stock market	Key management at user and CSP side
Content Sharing	Video-on-demand	Key management at user and Server side
Content Sharing	Google Docs	Key management at Service Provider side

Table.III Key management at various scenarios

Approach	Key management method	Key store	Features	Suitable Encryption key Method
Home based cloud	Key splitting Approach	For each member in the group, partial key will be stored at the user PC	Client requires less amount of memory to store the partial key, scalable security	Symmetric key for group
	Key management at server	For home based users that are not in the group are store key at its personal side		Asymmetric key for non-home users
	Key management at client	For non-home based users that are not in the group are store key at its personal side Public key stored at key server		
Out sourced private cloud	Key Splitting Scheme for customers in the group	For each member in the group, partial Key will be stored at the user PC	Client requires less amount of memory to store the partial Key	Symmetric key for group
	Key management at client	Private keys are accumulated at owners side		Asymmetric key for non-home users
		Public keys are accumulated at key server		
Onsite community cloud	Cloud server is deployed organization wide, beyond the boundary of organization should use Key management at centralized server	Key will be stored at the central server	As cloud is deployed in organization, more secure	Symmetric key
Outsource community cloud	Key management at customer and key management at server	Public Key accumulated in key server	Community organization get service from outsourced cloud	Asymmetric key
		Private key stored in mobile phones		
Public cloud	Key splitting Scheme for users in the group	For each member in the group, partial key will be stored at the user PC	Client requires less amount of memory to store the partial key	Asymmetric key
	Key management at client and key management at server	Private key stored in mobile phones and Public Key stored in key server	Security	

Table IV: Comparison of required key size for various schemes

Symmetric scheme(Key size in bits)	ECC based scheme (Key size in bits)	RSA(Key size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360