International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds

Vartika Srivastava
M.tech (Computer Science and engineering) from Buddha Institute of Technology (2018-2020) University- Dr. A.P.J Abdul Kalam technical University.

ABSTRACT

Over the most recent couple of years, Cloud figuring has increased a great deal of prominence and innovation investigators trust it will be the future, however just if the security issues are understood now and again. For the individuals who are new to distributed computing, it is a training wherein clients can get to the information from the servers that are situated in remote spots. Clients can do as such through the Internet to oversee, procedure and store the applicable information, rather than relying upon the PC or a nearby server. Numerous organizations and associations are utilizing distributed computing, which in the long run is quicker, less expensive and simple to keep up. Indeed, even the ordinary Internet clients are likewise depending on distributed computing administrations to get to their documents at whatever point and any place they wish. There are likewise various difficulties related with distributed computing like maltreatment of cloud administrations, information security and digital assaults. At the point when customers redistribute delicate information through cloud servers, get to control is one of the crucial prerequisites among all security necessities which guarantees that no unapproved access to made sure about information will be maintained a strategic distance from. Henceforth, distributed computing needs to assemble a component that gives protection, get to control difficulties and security to the client information. An appropriate and dependable encryption procedure with improved key administration ought to be created and applied to the client information before stacking into the cloud with the objective to accomplish made sure about capacity. It likewise needs to help record get to control and every single other document related capacities in an approach based way for any record put away in a cloud situation. This examination paper proposes a decentralized access control component for the information stockpiling security in mists which additionally gives unknown confirmation. This system permits the unscrambling of the put away data just by the legitimate clients, which is an extra element of access control. Access control component are decentralized which makes it vigorous when contrasted with concentrated access control plans implied for mists.

IndexTerms—Access control, validation, characteristic based marks, property based encryption, distributed storage.

1) INTRODUCTION

Distributed computing and capacity has accomplished the best quality starting at now in the specialized field. In present day business settings, the ascent sought after for information re-appropriating can be seen, which imprints to be the key association of corporate data. It is likewise used as a key advancement part behind different online affiliations for singular applications. These days, having a restricted amount of information proportional to 25 GB (1 TB at an extra cost), it is clearly not difficult to apply with the longing of complimentary records for electronic mail, mixed media stockpiling, document sharing or potentially remote access. Going connected at the hip with the ebb and flow day remote progression, information clients can get to the greater piece of their records and messages with a phone in any side of the universe

Thinking about the information security, a customary method to manage objective without question is to depend upon the server to favor the way control after assertion, which recommends any unforeseen preferred position speeding up will uncover all information. In a common residency scattered figuring condition, things wind up being essentially progressively genuine. Data from various customers can be put away and gotten to on various virtual machines (VMs) could conceivably be mounted on a particular physical machine. Information in an objective VM could be taken by starting up another VM on a similar machine as the objective one.

A made sure about server, notwithstanding giving a guaranteed stage that encourages the Web applications and web server configuration, likewise needs to answer the web

application's security. A server can incite unapproved get to. Overlooked customer records can permit an aggressor to hack your information without notice. Seeing the perils to your web server and having the ability to recognize appropriate countermeasures empowers you to speculate various security perils and upset the routinely creating amounts of gatecrashers.

The proposed application gives a bidirectional encryption of correspondences between a customer and server, which guarantees against listening covertly and playing with and additionally fabricating the substance of the correspondence. The application that the paper is set up to show up is to talk with and furthermore guarantee that the substance of understandings between the customer and the server can't be gotten to or produced by any aggressor. Any safe server in addition to application must have an essential two-way login security.

Clarifying in a word, in the wake of marking into the application customer gets a concealed key on his predetermined email id. This private key must be referenced in the content box gave during the time spent marking into made sure about server application. This application has two functionalities, Encryption and Decryption. Encoding is the value wherein the report to be standardized over the mail in initially changed over to byte design and adjust encoded using particular encryption computations. After Encryption records would be spared into the cloud database. At the shopper end, he will download the reports utilizing the application in the wake of being approved essentially by the KDC.

Customer security is additionally a compulsory in cloud. In any made sure about cloud application, the cloud or various customers don't have even the foggiest thought regarding the independence or personality of different customers. The immense stockpiling can hold the customer information and their solicitations in the cloud, and in the comparative way, to give benefits, the cloud itself is mindful. The validity of the customer who stores the data is likewise affirmed. This additionally determines the necessity of law approval for guaranteeing information security and assurance. Various encryption frameworks have been drilled to take care of data on cloud to scrutinize the information while doing figurings on the data. By using Attribute based encryption (ABE), the cloud gets the substance of the data, performs counts and passes the encoded arrangement of the conclusive outcome to the customer. The customer would then be able to decipher the result, in spite of the way that the cloud doesn't understand what data it has worked.

Various strategies have been proposed to guarantee the data substance assurance by methods for client control. Personality based encryption (IBE) was at first introduced by Shamir, in which the sender of a message can demonstrate a character to such an extent that only a recipient with planning personality can unscramble it. A pair of years afterward, Fuzzy Identity-Based Encryption is proposed, which is in any case called Attribute-Based Encryption (ABE). In such encryption technique, a personality is seen as a plan of clear qualities, and deciphering is possible if an unscrambled character has a couple of spreads with the one characterized in the figure content. After a short time, progressively wide tree-based ABE plans, Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher content Policy Attribute-Based Encryption (CP-ABE), are acquainted with express more point by point condition than obvious 'spread'. They are invariants to one another as in the decision of encryption procedure (who can or can't decipher the message) is set by different get-togethers

In KP-ABE, a figure content is related with a strategy of characteristics, and a private key is related with a monotonic access structure like a tree, which portrays this current client's personality (for example Unhitched males AND (Ph.D. Or then again Master)). A client can unscramble the figure content if and just if the path tree in his private key is happy with the references in the figure content. Regardless, the encoding plan is portrayed in the keys, so the scrambling client doesn't have all out power over the encoding approach. It needs to accept that the key generators issue keys with the correct structures to the correct customers. Moreover, when a re-encryption occurs, the vast majority of the hubs in a similar association must hold their individual keys, re-gave remembering the ultimate objective to mix to the re-encoded plates, and this strategy causes gigantic issues in the execution.

2) PROBLEM STATEMENT

The at present existing frameworks utilize a symmetric key methodology which doesn't bolster confirmation. The security saving access control proposed by Zhao for cloud information utilizes a brought together methodology where the keys and ascribes to the clients are disseminated by a solitary key conveyance community. In any case, this may be an issue if the KDC comes up short, which brings about the inaccessibility of the information to the cloud clients. Furthermore, it may build the heap on the KDC if the quantity of clients mentioning access to the cloud

information, applications and administrations is high. This may influence the exhibition of the KDC.

2.1 Objective

The essential target of this paper is to propose and construct an application that utilizes a decentralized access control component utilizing different KDC. The application additionally answers the issues of confirmation, security assurance, check of the information source by at first changing the content to figure and afterward producing the keys in a semi-down to earth design.

2.2 Noteworthiness of the Study

The proposed application actualizes Attribute Based encryption for elevated level information security, gives made sure about system engineering between proprietor, customer and cloud. It additionally permits the cloud servers to screen the client's confirmation even with no information on their character.

2.3 Extent of the Study

This extent of this paper is stretched out yet not constrained to building up an application for information stockpiling security usage in cloud systems. It additionally stretches out to have a more profound understanding on distributed computing and systems administration, to introduce a design utilizing Java as programming language lastly to examine the aftereffects of the functional usage versus hypothetical methodology.

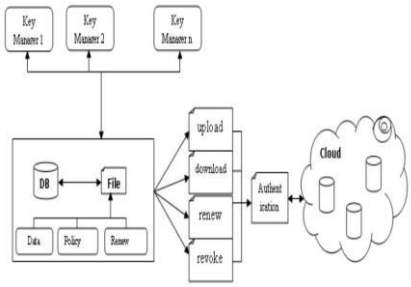

Figure 1: Overall System Design

The figure above clarifies the general framework configuration being proposed in this paper, all the included parts and the information stream between them. There are numerous Key Distribution Centers(KDC), the cloud where information records will be put away, the various clients, their validation levels and activities performed on the information.

3) LITERATURE REVIEW

3.1 Cloud Computing

In a layman's language, Cloud Computing can be characterized as one application being stacked which permits various clients to sign into an electronic application that has numerous other client programs. Remote machines would do everything from word handling to email to complex projects of information examination. A Cloud Computing framework is commonly partitioned into two sections, front end and back end. These both are associated through a system which is generally web. A general PC client or customer will be the front end and the cloud will be the back end. Internet browsers like Internet Explorer or Chrome are UIs and are considered as the front end. Different PCs, information stockpiling frameworks and servers join to make the back end "Cloud" figuring administrations and by and large every application is related with an alternate server.

3.2 Preferences of Cloud

A product called middleware is utilized to adhere to a lot of rules called conventions. The more the quantity of customers, the higher is the interest for information extra room and gadgets. A couple of reasons why businesses depend on Cloud figuring to store information and run the projects are as per the following:

Clients or customers can get to the applications and information from anyplace and whenever just by utilizing their PCs associated with the web. Thusly, the information access won't be limited to a specific hard drive, PC or a system.

Cost caused in acquisition of physical gadgets and propelled equipment can be diminished definitely. It requires just a screen, input gadgets like a mouse and console and some preparing capacity to run middleware and get associated with the cloud. No hard drive is required as all the information is put away in the cloud itself.

Organizations won't need to make a fuss over the most recent programming, its updates and permit buys. Distributed computing frameworks charge a metered expense and give all inclusive access to all the applications.

3.3 Access Control in Clouds

Client Based Access Control (UBAC): This is a strategy for security wherein the framework, applications and administrations are made sure about at individual or client level. UBAC, additionally referred to now and again as User based authorizations, is fundamentally executed as a basic login and secret key blend which either awards or rejects get to. UBAC improves granular control, yet with a high administration overhead as the progressions to any consent settings should be accomplished for each client. Organizations with high security concerns generally lean toward this sort of access control.

Job Based Access Control (RBAC): It is a technique for controlling access to framework, system or cloud assets dependent on the individual client jobs. Here, get to is characterized as the capacity to make, see or adjust a few information or play out some particular activity. Jobs might be characterized dependent on the duty or authority of a specific client. RBAC, when appropriately actualized, lets the clients do a wide scope of approved assignments by managing their activities as indicated by the limitations and connections progressively. In the RBAC, it is anything but difficult to make, change or erase the jobs according to the necessities indicated by the customers.

Trait Based Access Control (ABAC): This is a discernable access control component where access to the framework or administrations in the cloud is conceded subsequent to assessing certain standards against the qualities of the substances. Traits might be characterized as an impressive trademark to which a worth can be allocated. Fundamentally, ABAC depends on the assessment of properties of the subjects and items, condition conditions and the entrance control rules characterizing the adequate activities for subject-object qualities. ABAC frameworks are fit to implement both Discretionary Access Control (DAC) and Mandatory Access Control (MAC). [Li, J., Ren, K., Zhu, B., and Wan, Z. (2009)][Cui, B., Liu, Z., and Wang, L. (2015)]

3.4 Cryptography

As indicated by The NIST Computer Security Handbook [NIST95], the term PC security is characterized as "The assurance stood to a mechanized data framework so as to accomplish the relevant targets of saving the respectability, accessibility and classification of data framework assets (incorporates equipment, programming, firmware, data/information, and media communications)." The procedure or technique that ensures the data and administrations are being defended from unapproved access, control or alteration and pulverization can be authored as security system. By and large, this security in systems administration where information will be moved over conventions will be depended upon Cryptography. Cryptography is a word gotten from Greek language signifying "Mystery Writing", in different ways, a specialty of making messages made sure about against outside assaults by changing them.

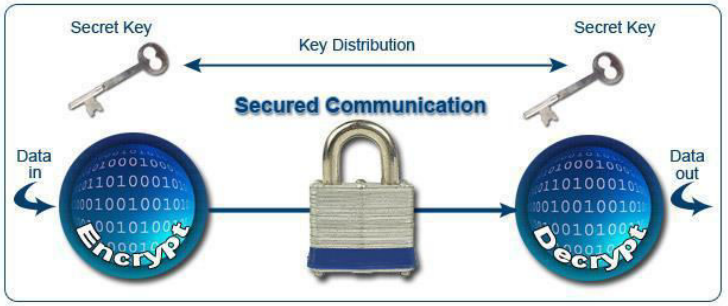

Figure 2: Cryptography Overview

Encryption can be referenced as one of the most dependable approaches to guarantee that the data affectability is protected. All the surely understand encryption calculations accessible in the present day for any data security change the plain content into figure message by applying various changes, replacements or both in equal. The plain content is the first information and the figure content is the aftereffect of applying the encryption approachs to the plain content. The figuring out of encryption is called unscrambling where in certain approachs are applied on the figure content to recover the plain content. These encryption calculations are arranged into Symmetric and Asymmetric dependent on the keys being utilized for encryption. Symmetric encryption calculations, likewise called as ordinary encryption calculations are those which utilize a similar key for both the encryption and unscrambling forms. Thus, hilter kilter encryption calculations are those in which two unique keys, open and private keys are utilized for encryption and unscrambling.

3.5 RSA Algorithm

RSA, planned in 1978 was named after its creators Ron Rivest, Adi Shamir and Leonard Adleman. It is known to be outstanding amongst other open key encryption

calculations till date for key age, encryption, decoding and advanced marks. The encryption squares and the key in RSA are of variable sizes. RSA is a topsy-turvy calculation relying upon the number hypothesis. The general population and private keys are produced utilizing prime numbers which are later utilized for encryption and decoding. The information sender utilizes the recipient's open key to encode the information and send it, while the information collector utilizes his own private key to unscramble the information and access it. The entire RSA procedure can be conveyed into three stages like key age, information encryption and unscrambling.

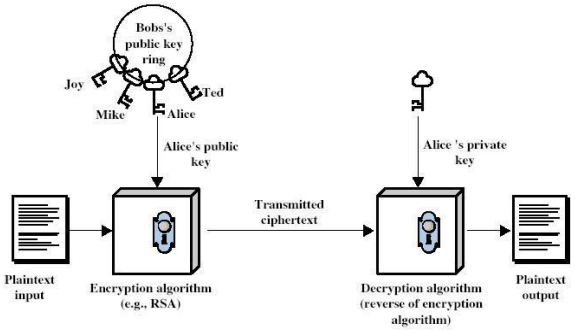

Figure 3: Public Key Cryptography.

The RSA works this way:

Alice picks two huge primes pA and qA.

Alice registers n A = pA qA and ϕ(n A) = (pA–1)(qA–1)

Alice picks a whole number eA with gcd(eA,ϕ(n A)) = 1, conceivably at arbitrary.

Alice registers dA ≡ eA −1 (mod ϕ(n A)).

Alice's open key is (n An, eA). She appropriates this. Her private key is dA. She stays quiet. Alice can dispose of pA, qA, and ϕ(n A).

On the off chance that 2k ≤ n A < 2k+1, Alice's capacity of encryption for short messages (k bits or even less, so M

< n An) is: EA(M) = MeA (mod n A). Anybody can process EA (M). A long message is scrambled by parting it into k-bit squares, and encoding each square independently. Note that each encoded square has k+1 bits.

Alice's decoding capacity for short messages is: D A(M) = MdA (mod n A), given 0 ≤ M < n A. Nobody else other than Alice (or other people who has Alice's private key) can register this. Note: D A (EA (M)) ≡ (MeA) dA ≡ MeA dA ≡ M (mod n A) since eA dA ≡ 1 (mod ϕ(n A))

When Alice has done this, she can Receive messages that are encoded from Bob (or others), and

Send carefully marked messages to Bob (or any other person). On the off chance that Alice needs to send encoded writings to Bob, or to get carefully marked writings from Bob, Bob should pick his own open and private keys, (nB, eB) and dB. Bounce sends a short message M (at most k bits) to Alice like this:

i) Bob scrambles M as MeA (mod n An), and sends MeA to Alice. (Note Bob knows eA and n An.)

ii) Alice unscrambles MeA as (MeA) dA ≡ M (mod n A). Accordingly Alice recuperates M. (Note Alice really recoups the estimation of M (mod n A), however this is proportionate to M fulfilling M < n A.) For huge messages, Bob could isolate the message to k-bit squares, and scramble independently every square. Alice would isolate the message that is encoded in k+1 bit squares, and decode independently every square. [Behrouz A Forouzan, "Systems administration and Data Communications"]

3.6 Data Encryption Standard (DES)

DES, an encryption calculation that has been created in the mid-1970's, has picked up the best standard by the National Institute of Standards and Technology (NIST). It was likewise embraced worldwide by different areas of governments. It was constantly given a high need with regards to the money related industry. It is a square figure and uses a square size of 64 bits. The key size is 56 bits and 8

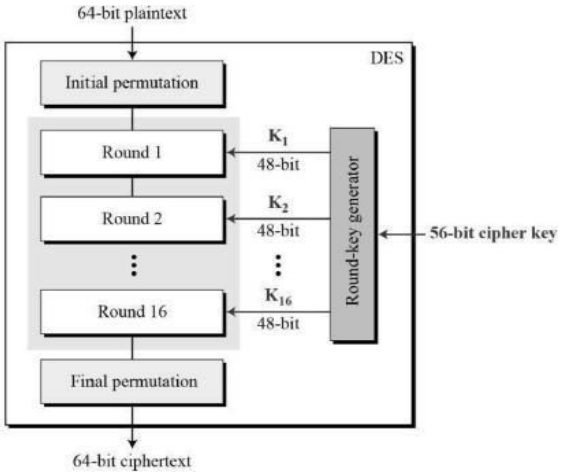

Figure 4: DES Algorithm

bits will be utilized for equality. This setup of the calculation makes it powerless to thorough quest for keys for the present day PCs and extraordinary equipment. DES is supposed to be effectively weak with the assistance of extraordinary equipment utilized by criminal associations, governments or significant enterprises, and yet sufficient against the irregular hacking procedures. It isn't being utilized nowadays for any new applications as it is getting more vulnerable.

One other variation of DES called TRIPLE-DES (3DES) has been presented later. This calculation works by applying DES in three phases with various keys for each stage. The length of the key in 3DES would inevitably become 168 bits. Regardless of being a lot more grounded than DES, 3DES is moderate when contrasted with some other square figures recently developing. DES and its variations are as yet viewed as significant, regardless of whether it appears to seem as though having less keen on the present applications. DES, as the first since forever square figure assumed a significant job in giving the open solid cryptographic calculation and was thus conveyed generally in the open segment.

3.7 Advanced Encryption Standard (AES)

In 2001, NIST suggested AES as the most recent encryption standard that replaces the DES calculation. AES calculation bolsters numerous mixes of information like 128, 192, 256 bits, and so on. Contingent upon the length of the key utilized in encryption or decoding procedures, the DES calculation is named as AES128, AES 192, and AES256. The quantity of rounds in encryption and decoding process contrast in DES calculation dependent on the length of the key. AES has 10, 12, 14 rounds for 128, 192, 256 bits separately. These rounds accept the plain content as info and produces the last figure message as yield. In AES, the 128 piece information square is apportioned into four separate operational squares where each square speaks to a variety of bytes. These varieties of bytes are organized in a framework type of 4 lines and 4 sections that is named as a state. In either encryption or unscrambling strategies, the primary activity that happens is an Add Round Key. In the following stage, the yield experiences nine additional means where each round includes four distinct changes of information. These changes incorporate Sub-bytes, Shift-lines, Mix-sections, Add Round Key. No Mix-Column change happens in the last tenth round. The beneath figure represents the total change and encryption process. The unscrambling procedure is same as encryption process in AES aside from that the arrangement of steps is turned around and reverse capacities like Inverse Sub-byes, Inverse Shift Rows, Inverse Mix-Columns, and Inverse Add Round Key are utilized. Every single other advance continue as before.

4. SYSTEM ANALYSIS

4.1 Existing System

Data get to control ends up being a high need issue in dispersed capacity frameworks when the data is re-appropriated to the cloud servers that are un-trustable. The current access control plans appear to be unseemly as they require a total, confided in cloud server or they produce mixed copies. Much more, they depend on a solitary KDC for all the entrance key solicitations from various clients.

In any situation, the information proprietor won't be concerned or connected with the procedure that the information director gives information access to the information shopper in the present disseminated stockpiling organization frameworks. Furthermore, when this framework depends on un-confided in cloud servers, the information get to control will be an issue to be tried and taken extra consideration. Also, consequently, it is not any more suitable to utilize the ordinary server-based access control methods for circulated capacity frameworks.

4.2 Proposed System

In the proposed application framework, Attribute Based Encryption is utilized to have the data in memory to be mixed to the absolute last piece. The application permits cloud servers to control both the proprietors and clients get to authorizations, even without knowing their character data. It guarantees that the customer's security in defended in every single imaginable ways.

The proposed application has both encryption and decoding functionalities. As a component of encryption, the document that must be made sure about is previously partitioned into four comparable estimated byte game plans and afterward encoded utilizing the AES encryption calculation. After encryption, the records will be put away in the cloud. At the client end, the record would be downloaded once the client gets confirmed by the KDC with the proprietor key and n-authority key, utilizing which the document will be decoded. All the secret key validation and access key correspondence are done through Gmail

utilizing the mail tends to given by the clients during the enrollment.

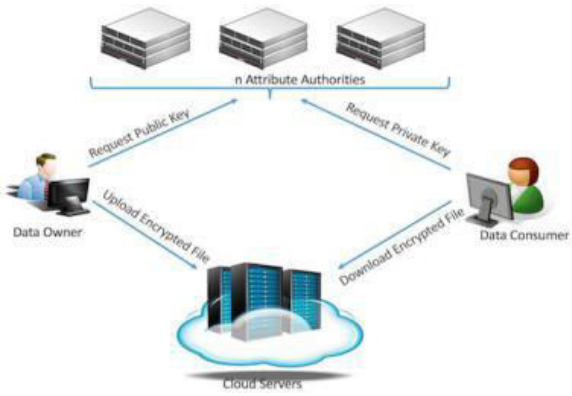

Figure 5: Overall System Flow

5. IMPLEMENTATION

The principle jobs in the application actualized are the information proprietor, information customer, cloud administrator and the n-Key position (KDC). All these have their functionalities which are portrayed as follows according to the work process usage.

5.1 Data Owner

The customers or the clients who might want to spare their information records in the cloud in a protected and secure way make the information proprietors segment. These information proprietors register in the application by giving all the essential subtleties and from that point login with the got secret word. When the proprietor signs in, he can demand the KDC for a quality key which is required for him/her to transfer the record he/she wishes to. The document that has been transferred can be scrambled lastly transferred in the cloud database. The proprietor is furnished with a choice to scramble the document for the subsequent time dependent on his prerequisite.

5.2 Data Consumer

The genuine clients who wish to devour the information that is put away in the mists contain the information buyer segment of the application. Like the information proprietors, the information shoppers likewise need to enroll themselves by giving all the necessary data and enlisting. At that point after, they have to pick the record that they need to download and demand the KDC for the entrance key to do as such. When the shopper presents the equivalent in the application, he/she will be permitted to download the document after it is unscrambled utilizing the keys submitted.

5.3 Cloud Server

The cloud server stores the data of the information proprietors just as the information customers and offers access to them on the documents as per their authorizations. It distributes explicit ids for the documents being put away in it and accordingly makes it simpler for the clients to pick which record to download. It creates the unscrambling tokens of a figure content for the clients by using the keys of the clients produced by the KDC.

5.4 The Public Cloud

An open cloud is a mutual one which can be gotten to by each and every individual who utilizes a web association or a Visa by paying according to use with no membership. Subsequently open mists have a virtualized framework that is normally shared by a few unique clients. They are open effortlessly and can be overseen from a devoted self-administration gateway.

5.5 The Private Cloud

A private cloud is available just to explicit clients. In a private cloud, the administrations and foundations are overseen on a private system. In contrast to an open cloud, a private cloud is overseen and claimed secretly. Its entrance is confined to a solitary or part of a business. As far as dependability, security, information persistency and protection, a private cloud appears to be a lot more secure to associations.

The Hybrid or Mixed Cloud A Hybrid or Mixed cloud is a blend of private and open cloud. It incorporates the benefits of both private and open cloud for an organization.

5.6 The Community Cloud

A Community Cloud is explicitly utilized by an expert network that may incorporate subcontractors or accomplices who work cooperatively on a similar undertaking or a cloud devoted to government or state establishments.

5.7 Key Distribution Center

KDC is a self-sufficient quality power place that stays responsible for giving, disavowing and overhauling the

clients' approaches by part or character in its region. In DACMACS, every quality is associated with a single KDC, anyway every KDC can manage an optional number of properties or traits. Each KDC has full power over the structure and semantics of its properties. Each KDC is responsible for making an open property key for each trademark it administers and an entrance key for each customer band together with their properties.

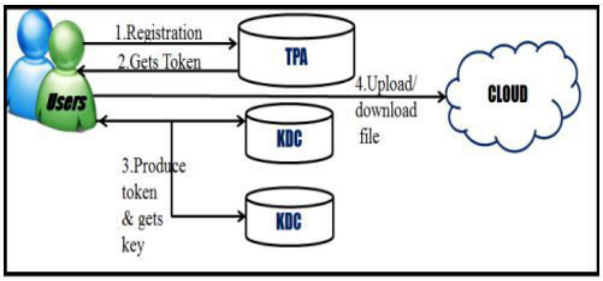

Figure 6: KDC Architecture

For guaranteeing the exactness of information that is put away in the cloud server, we have planned a framework that approves the rightness of the information put away alongside maintaining a strategic distance from the framework social errors. Accuracy of information put away. In any conditions, the framework is intended to guarantee that suitable and important information is put in the cloud. It additionally keeps the information put away in cloud intact all the occasions. Quick confinement of mistake information. In any event, when the server disappointments happen, the structured framework progressively fixes or alters the server regardless of the sort of disappointment so as to keep the information from being lost or adulterated or harmed.

Dynamic tasks backing of information. The proposed framework underpins all the dynamic tasks at whatever point the client changes the information by playing out any activities like supplement, annex, erase, and so forth. Constancy. The framework created is away from conditions. It diminishes the impact of server disappointments or information blunders and in this way defends the information from the sudden disappointments, noxious dangers, unapproved information changes, server conspiring assaults, and so forth. Lightweight correspondence. This structure likewise permits the clients to perform security checks to confirm if the information put away is right and not debased without least cost. The engineering structured confirms clients and empowers them to stay mysterious while utilizing the cloud. Numerous past usage give just paired aftereffects of the information stockpiling state among different disseminated servers, yet our framework furnishes confinement of blunder information alongside twofold outcomes. The beneath figure delineates the design of run of the mill Key Distribution Center utilized in our proposed framework. Any client who claims a lot of documents, stores them in the cloud server in scrambled structure and by utilizing ordering.

At whatever point the client signs into the framework, two stages of confirmations occur. One is with TPA (Trusted Party Authenticator) and the other with the KDC (Key Distribution Center). It includes the accompanying activities:

Administration Request to TPA. At first, any new client needs to get enrolled into the framework by entering his first name, last name, telephone number, email, username, and so forth. The client registers with his/her unique personality and approves his character against TPA. For enlistment, the client sends a solicitation to TPA. After effective enlistment, he/she gets an email with a brief secret phrase which he can change anytime of time by utilizing "Change Password" choice. Every single existing client can legitimately login into the framework without enrolling.

6. CONCLUSION

In the proposed paper, the thoughts of different encryption techniques like IBE, ABE, KP-ABE, and CP-ABE are examined with subtleties of their favors and furthermore bothers. Different symptoms with the brought together methodology of access control systems have been laid out. Additionally, the advantages of the decentralized access control system have been clarified which utilizes different KDC engineering with unknown confirmation. An arrangement has been laid, explored upon, examined and disclosed on the best way to assemble an application that answers the disseminated get to control instrument in the cloud design with unknown validation.

6.1Results and Conclusion

As proposed and arranged, an application has been created satisfying all the necessities. Extraordinary consideration and fixation has been placed in the entire procedure beginning from picking the advancements, breaking down the connections and suggestions, creating and testing the application thoroughly. The final product was appeared as screen captures. All the fundamental testing has been to done to guarantee the usefulness. The application is

executed in the neighborhood databases and saw as better near to the concentrated access control system.

References

[1] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), May 2011.

[2] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, April 2001.

[3] X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 210-227, May 2007.

[4] D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 257-265, May 1991.

[5] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, June 2008.

[6] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, April 2011.

[7] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, April 1996.

[8] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, May 2005.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, May 2006.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, June 2007.

Curriculum Vitae

Name : Vartika Srivastava
Academic Details –
1) Pursuing M.tech (Computer Science and engineering) from Buddha Institute of Technology (2018-2020) University- Dr. A.P.J Abdul Kalam technical University.
2) B.tech (CSE) in 2018 from Kanpur Institute of Technology