International Journal of Database Theory and Application
Vol.9, No.11 (2016), pp.137-148
http://dx.doi.org/10.14257/ijdta.2016.9.11.13

Key Aggregate Based Homomorphic Encryption for Efficient Authentication for Secure Cloud Storage

K Ruth Ramya[1], D Naga Malleswari[1], Ch Radhika Rani[1],
Debnath Bhattacharyya[2] and Hye-jin Kim[3]

[1]Department of Computer Science and Engineering,
[2] Department of Computer Science and Engineering,
3Sungshin Women's University
KL University, Vaddeswaram, AP, 522502, India
Vignan's Institute of Information Technology,
Duvvada, Visakhapatnam, India
2, Bomun-ro 34da-gil,
Seongbuk-gu, Seoul, Korea
ramya_cse@kluniversity.in, debnathb@gmail.com, hyejinaa@daum.net
(Corresponding Author)

Abstract

Now a day's data out sourcing is the main focusing term in real time cloud computing applications. Secure data outsourcing is another real time intellectual concept in cloud computing applications for proceeding efficient data transmission. Conventionally Attribute Based Encryption (ABE) performs efficient data security of data outsourcing in cloud. It performs effective data security based on attributes of uploaded data for storage. Attributes are key terms for converting plain file data to Meta (cipher) file, so every time attribute extraction is complexity in data storage in cloud for efficient security analysis. We describe new public cryptographic system which effects fixed size for efficient delegation of decryptions for cipher-texts. So in this paper we propose to KAE (Key Aggregate Encryption) for efficient data security for providing. The novelty is one can aggregate any set of secret keys and make them as complete with single key with power of all the keys been aggregated. We provide security analysis as a development in real time cloud applications for processing access control data delivery between users present in cloud. Our experimental results show efficient security with access control policies in data storage in cloud.

***Keywords**: Cloud Computing, Attribute based encryption, Scalable and reliable data encryption and decryption, secure Hashing*

1. Introduction

Cloud computing is innovative network access to share services with different users in computer resources. In cloud computing achieves storage alternatives provide different customers with various abilities to store and share user's information in third party information facilities. In real time configurations it depends on discussing of various of sources of coherence with financial system with range of similar applications. At the base of cloud computing applications incorporated facilities and distributed services with proceedings in real time configurations.

ISSN: 2005-4270 IJDTA

MOBILE
WEB
NETWORK
CLOUD SERVICES
APPS
SERVER
DATABASE

Figure 1. Cloud Computing Services in Resource Monitoring

As shown in the Figure 1 cloud computing provides three types of solutions regarding thinking support and other proceedings present in distributed handling functions. SAAS(Storage As a Service), PAAS(Platform As a Service), and Facilities As a Service are three solutions of the thinking handling for storage space information, handling information and preserves of information which includes all the activities of the customers presentation may appears recent development of information motivation program [2]. Consider the examples of Mediafire.com, SendSpace.com and Amazon Cloud Web solutions and other solutions are storage space of information in thinking and other continuing website signing up procedure. These are the successive web sites for providing solutions to various customers for storing their information with handling program. Reasoning contains share of solutions of details. All kinds of customer demands are applied with good performance and interaction expense contains high. Protection and comfort signify major issues in the adopting of reasoning technological innovation for information storage. A strategy to minimize these issues is the use of security. However, whereas security guarantees the privacy of the information against the reasoning, the use of conventional security techniques is not sufficient to support the administration of fine-grained business Access Control Policies (ACPs). Many companies have today ACPs controlling which customers can accessibility which data; these ACPs are often indicated in terms of the qualities of the customers, generally known as identification features, using accessibility management languages such as XACML. Such an strategy, generally known as Attribute-Based Accessibility Controllability (ABAC), facilitates fine-grained accessibility management which is crucial for high-assurance information security and comfort.

Attribute-Based Encryption (ABE) allows only organizations having a specified set of features can decrypt cipher texts [3-4]. ABE is appropriate to accessibility management such as the computer file discussing techniques, because several organizations can be provided for the decryption of a cipher text. We have been suggesting an enhanced ABE plan that is more effective than past one. Through present delegate calculations we are going to consume the solutions usage with new security difficulties execution procedure. In the storage space service program, the reasoning can let the customer, information proprietor to shop his information, and discuss this information with other customers via the reasoning, because the reasoning can provide the pay as you go atmosphere where people just need to pay the money for the storage space they use. For defending the privacy of the saved information, the information must be secured before posting to the reasoning. The security plan used is attribute-based security. The ABE plan used a customer's identification as features, and a set of features were used to secure and decrypt information. One of the main efficiency disadvantages of the most current ABE techniques is that decryption is costly for resource-limited gadgets due to coupling functions, and the number of coupling functions required to decrypt a cipher written text develops with the complexness of the accessibility plan. The ABE plan can outcome the issue that information proprietor needs to use every approved customer's community key to secure information.

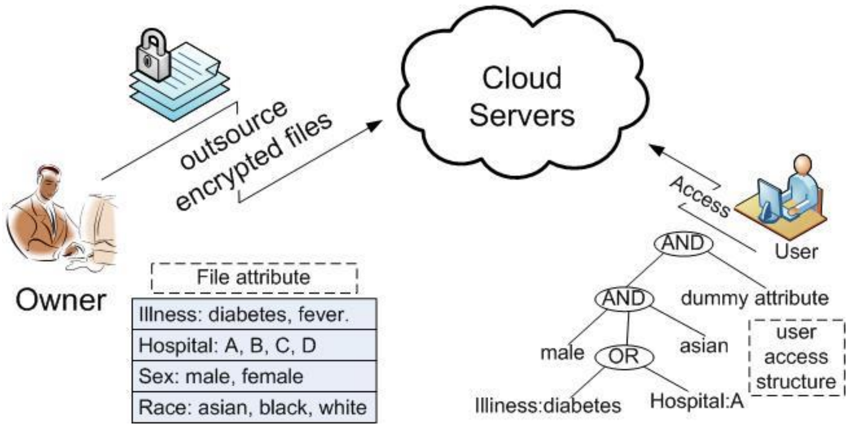

Figure 2. Attribute Based Encryption for Outsourcing Data [2]

Trust that Alice areas all her individual pictures on Fall Box, and she wouldn't like to demonstrate her photos to everybody. Because of different points of interest stream plausibility Alice can't experience took care of by simply construct upon in light of agreeableness insurance frameworks gave by Fall Box, so she scrambles all the photos utilizing her own particular key components before distributed. One day, Alice's companion, Bob, requests her to discuss the photos assumed control over every one of these years which Bob showed up in. Alice can then utilize the discussion about capacity of Fall Box, yet the issue now is the means by which to allot the decoding benefits for these photos to Bob. A conceivable alternative Alice can choose is to safely give Bob the key components included. Ordinarily, there are two compelling method for her under the standard insurance worldview:

Alice encodes all information documents with stand out security key and gives Bob the comparing key straight.

Alice encodes information records with extraordinary essential elements and conveys Bob the comparing key vital variables.

As appeared in Figure 3, clearly, the primary system is deficient since all unchosen information might be additionally discharged to Bob. For the second strategy, there are practical issues on execution. The quantity of such critical variables is the same number of as the assortment of the mutual pictures, say, a million. Moving these mystery keys typically needs an ensured course, and putting away these critical components needs rather costly secured storage room [6]. The costs and issues included more often than not upgrade with the quantity of the decoding key components to be designated. In a nutshell, it is vast and unreasonable. Assurance key components likewise accompany two inclinations-symmetrical key or hilter kilter (open) key. Utilizing symmetrical encryption, when Alice needs the points of interest to be slides from an outsider, she needs to give the encrypt or her key; clearly, this is not generally proper. By examination, the insurance key and decoding key are distinctive in broad daylight key security. The utilization of open key encryption gives more adaptability for our applications. For instance, in business alternatives, each worker can distribute secured insights about the reasoning stockpiling range space server without the points of interest of the organization's lord mystery key.

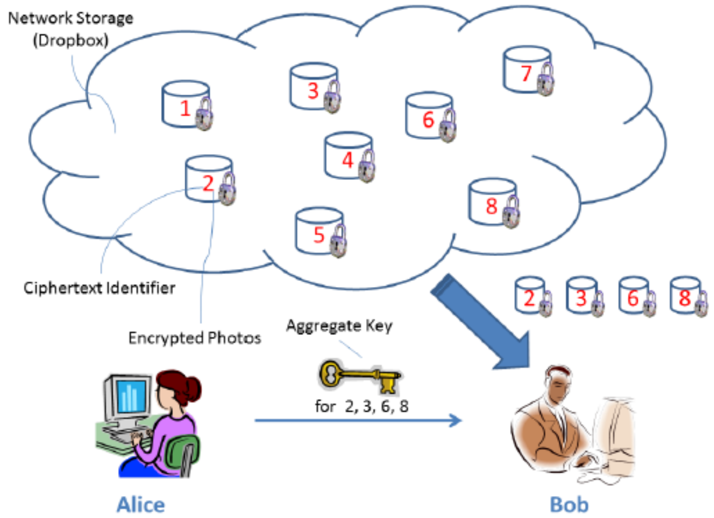

Figure 3. Alice Stocks Information with Identifiers 2, 3, 6 and 8 with Bob by Delivering him Only One Total Key

In this manner, the best treatment for the above issue is that Alice encodes data with special open keys, however just gives Bob one and only (steady size) decoding key [8]. Since the decoding key ought to be sent by means of an ensured course and kept key, minimal key measuring is constantly fitting. For instance, we can't foresee tremendous storage room for unscrambling key components in the asset imperative devices like advanced cells, splendid bank cards or remote interchanges.

Particularly, these key components are generally put away in the carefully designed storage room, which is moderately costly. The present examination extends predominantly concentrate on lessening the associations necessities, (for example, band-with use, units of correspondence) like aggregate mark.

The remaining of this paper organized as follows: Section II provides overview of the related work presented in previous application procedures, In Section III present Traditional approach with security considerations; Section III describes effective data presentation and construction of the proposed approach. Section IV analyzes the security cloud with flexible and effective computation with real time performance evaluation and implementation. Section V describes concluded process of cloud security process.

2. Background Approach

Normally see framework particular control highlight based security contracted blueprint was displayed Contrary to the configuration for ordinary ABE, a KGSP and a DSP are moreover included. . KGSP is to perform keyed issuing calculations to decline AA finish a reach project when a great deal of clients make necessities on individual key creation and key-overhaul.

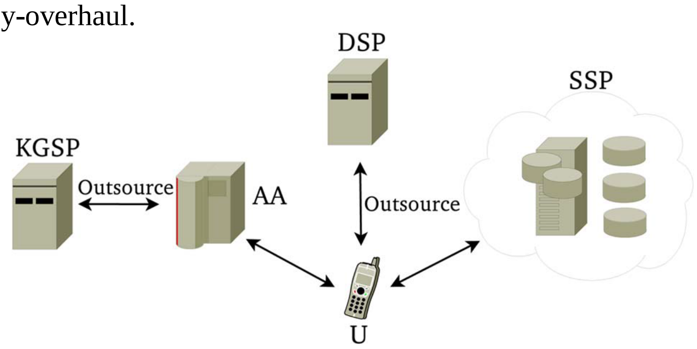

Figure 4. Data Outsourcing Model Using ABE

DSP is to finished assigned costly components to get over the weakness that the unscrambling level in common ABE needs a great deal of undesirable elements at U.

Using some of the key demonstration over approximated on the out seeking information with reflection of the secured key with information discussing and other resources using reasoning processing secured solutions such as dedication and other source solutions. We represent (Ienc; Ikey) as the feedback to security and key growth [13-14]. In CP-ABE plan, (Ienc; Ikey) = (w, A) while that is (w, A) in KPABE, where w and A are function set and availability structure, respectively. Then, depending on the recommended system style, we provide requirements details as follows:

Setup (μ): The set up requirements needs as feedback V a security parameterseter μ. It results a group key PK and a professional key MK.

Key Gen init (Ikey; MK) : For each user's individual key demand, the initialization requirements for assigned key growth needs as feedback Van availability strategy (or feature set) Ikey and the professional key MK. It results the key several (OKKGSP; OKAA) [2].

Key Gen out (Ikey; OKKGSP): The allocated key creation criteria needs as feedback the availability structure (or function set) Ikey and the key OKKGSP for KGSP. It results a restricted adjustment key TKKGSP.

Key Gen in (Ikey; OKAA): The within key creation criteria needs as feedback the availability structure (or feature set) Ikey and the key OKAA for feature power. It results another restricted modification key TKAA.

Key Sightless (TK): The advance key stunning criteria needs as feedback V the adjustment key TK (TKKGSP; TKAA). It results a individual key SK and a diverted adjustment key f TK.

Secure (μM; Ienc): The security prerequisites needs as input V a thought M and a capacity set (or openness structure) Ienc to be appropriately secured with. It comes about the figure composed content CT.

Decode out(CT; f TK) : The allotted unscrambling criteria requires as input V a figure composed content CT which was accepted to be legitimately secured under the capacity set (or openness structure) Ienc and the redirected adjustment key f TK for accessibility structure (or capacity set) Ikey. It comes about the incompletely unscrambled figure content CT part if (Ikey; Ienc) ¼ 1, generally comes about?, where μ is a predicate pre-indicated.

Decode (CT part; SK): The unscrambling requirements requires as information V the incompletely unscrambled figure content CT part and the individual key SK. It comes about the special thought M [2].

Consider the above procedure of secured data outsourcing in thinking may execute powerful process for security in data proceeding of most recent strategies. Secure outsourcing ABE framework which helps both secured abbreviated key-issuing and unscrambling. Our new technique offloads all accessibility procedure and capacity suitable components in the key-issuing procedure or decoding to a Key Creation Assistance Organization (KGSP) and a Decryption Assistance Organization (DSP), individually, making just a progressing number of straightforward elements for the capacity control and affirmed customers to execute locally. Also, interestingly, we recommend a contracted ABE development which gives check ability of the abbreviated calculations results in a viable way. Thorough security and execution investigation demonstrate that the prescribed techniques are checked secured and reasonable. Effective Hierarchal structure of the accessibility control using feature based encryption (ABE), better system was needed for during above concerns successfully.

3. Key Generation Encryption

We first convey the abode and centrality for key complete assurance. At that point we depict how to utilize KAC in circumstances of its framework in speculation stockpiling region space.

Structure: A key-total assurance arrangement contains five polynomial-time procedures as takes after:

The subtle elements proprietor chooses town framework parameters through SETUP and is an open/expert mystery key couple by means of Key Gen. Data can be appropriately secured by means of Secure by any individual who likewise chooses what figure discharged composed content characterization is connected with the basically discharged composed content to be legitimately secured [8-9] The points of interest proprietor can utilize the expert mystery to deliver a complete unscrambling key for an arrangement of figure discharged content sessions through Remove. The made key components can be acknowledged to partners safely (by means of legitimately secured messages or appropriately secured gadgets) Lastly, any customer with a complete key can unscramble any figure discharged composed content given that the figure content's characterization is incorporated into the complete key through Decrypt.

Shared Secured Data: Here we depict the principle thought of subtle elements discussing in speculation stockpiling zone space utilizing KAC, demonstrated in decide 3. Expect Alice needs to discuss her points of interest m1; m2; : ;m on the server. She first performs Installation (1λ; n) to get parameters and perform Key Gen to get the general population/expert mystery key couple (pk; msk). The framework parameters and open key pk can be discharged and ace mystery key msk ought to be kept key by Alice. Anybody (counting Alice herself) can then legitimately secured every mi by Ci = Secure (pk; i; mi). The encoded points of interest are exhibited to the server. With parameters and pk, individuals who work with Alice can upgrade Alice's points of interest on the server. When Alice will discuss a set S of her points of interest with somebody Bob, she can ascertain the complete key KS for Bob by executing Extract (msk; S). Since KS is only a proceeding with measurement key, it is conceivable to be sent to Bob through a legitimately secured email. In the wake of acquiring the complete key, Bob can get the subtle elements he qualifies to accessibility [10]. That is, for every i 2 S, Bob introducing Ci (and some required ideas in parameters) from the server. With the complete key KS, Bob can unscramble every Ci by Decrypt (KS; S; i; Ci) for every i 2 S.

4. Implementation of KAC

Let G and GT be two cyclic categories of primary purchase p and ^e: be a map with the following properties:

Bilinear:

$$\forall_{f1,f2} \in \mathrm{A}, a, b \in \mathrm{M}, \hat{e}(f\ ,f\ ) = \hat{e}(f1, f2)^{ab}$$

Non-degenerate: for some $f \in \mathrm{A}, \hat{e}(f, f) \neq 1$. G is a bilinear team if all the functions engaged above are effectively computable. Many sessions of elliptic shapes function bilinear categories.

4.1. Construction

The style of our essential arrangement is propelled from the agreement safe transmitted security arrangement recommended. Despite the fact that their arrangement encourages consistent size key imperative components, each key just has the vitality for decoding figure instant messages related to a specific index [8]. We in this manner need to build up another Draw out criteria and the relating Decrypt criteria.

Setup: Arbitrarily choose a bilinear team G of primary order p where $2^{\lambda} \leq p \leq 2^{\lambda+1}$ a generator $f \in \mathrm{A} and \alpha \in_R \mathrm{M}_p$. Compute $f_i = f^{\alpha^i} \in \mathrm{A}$ for $i = 1, \ldots., a, a+2, \ldots., 2a$. Output parameter as $param = (f, f1, \ldots.., f_n, f_{n+2}, \ldots.., f_{2n})$ Observe that each cipher text category is showed by an index in the integer set $i = 1, \ldots., a, a+2, \ldots., 2a$, where n is the maximum variety of cipher text classes.

Key Gen: Pick $\gamma \in_R □_p$ output the public and master secret key pair : $(pk = v = g^{\gamma}, msk = \lambda)$.

Encrypt: For a message $m \in \mathrm{A}_T$ and an index $i \in \{1, 2, 3, \ldots...n\}$ randomly pick $t \in_R \mathrm{M}_p$ and compute the cipher text $e = (f^t, (vf_i)^t, m.\hat{e}(f1, fm)^t)$.

Decrypt ($K_s, S, i, e = (c1, c2, c3)$**):** If $i \notin S$ output is λ otherwise

$$m = c_3.\hat{e}(K_s.\prod_{j \in s, j \neq i} f_{n+1-j+i}, c_1) / \hat{e}(\prod_{j \in s} f_{n+1-j}, c_3)$$

4.2. Performance

For insurance, the quality ^e(f1; fn) can be pre-figured and put in the system parameters. In any case, we can see that decoding just requires two pairings while one and only of them incorporates the aggregate key [12]. That implies we just need one coupling figuring's inside the assurance processor sparing the (mystery) all out key. It is quick to gauge a coupling nowadays, even in asset obliged gadgets. Successful application executions exist notwithstanding for pointer hubs.

4.3. System Process

The "magic" of getting constant-size total key and constant-size cipher written text at the same time comes from the linear-size system parameterseter.

Our motivation is to diminish the ensured storage room and this is an exchange off between two sorts of storage room. The parameters can be set in non-secret neighborhood storage room or in a capacity reserve offered by the organization. They can likewise be gotten on prerequisite, as not every one of them is required in all occasions. The framework parameters can likewise be created by a trusted festival dispersed between all clients and even hard kept in touch with the client framework (and can be changed by means of "patches"). For this situation, while the clients need to have confidence in the parameters-generator for securely taking out any vaporous qualities utilized, the availability control is still guaranteed by a cryptographic mean as opposed to relying upon some server to constrain the gets too truly.

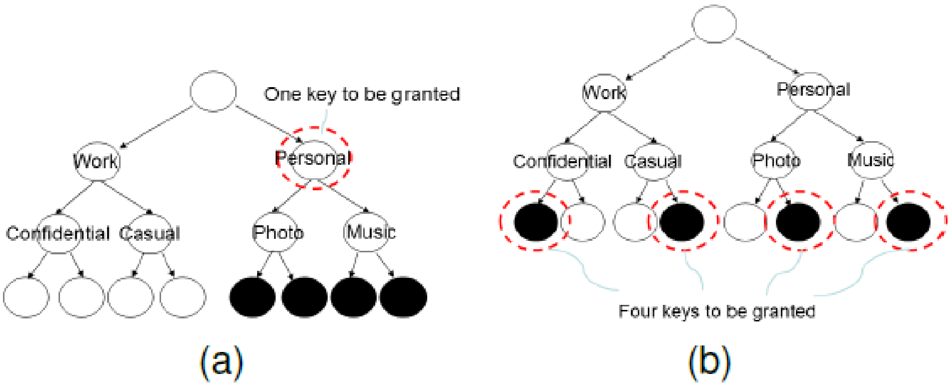

Figure 5. Compact Key is not Always Possible for a Fixed Hierarchy

5. Performance Evaluation

For a solid evaluation, we dissect the spot prerequisites of the tree-based key procedure strategy. This is utilized as a part of the Finish Sub bush procedure, which is a subsidiary answer for the event on security issue taking after the understood Subset-Cover structure [13]. It keeps running on the set sensible key system, which is appeared with a broad paired key plant of estimating h (equivalents to 3 in decide 4), and in this way can bolster up to 2h figure distributed composed content sessions, a chose part of which is made for an acknowledged allocate.

In a perfect situation as spoke to in Figure 5(a), the appoint can be offered the accessibility 2hs sessions with the having stand out key, where hs is the measuring a specific sub plant (*e.g.*, hs = 2 in Figure 5(a)). On the other side, to decode figure sms data of an arrangement of sessions, in some cases the allocate may need to keep an immense number of key components, as spoke to in decide 5(b). Along these lines, we have an enthusiasm for na, the extensive variety of symmetric-keys to be doled out in this requested key procedure, in a standard sensation.

We trust that there are precisely 2h figure distributed composed content sessions, and the dole out of issue permitted to a segment r of them. That is, r is the appointment sum, the quantity of the doled out figure distributed composed content sessions to the entire sessions. Clearly, if r = 0, Na ought to likewise be 0, which suggests no accessibility any of the classes; if r = 100%, Na ought to be as low as 1, which demonstrates that the having just the essential key in the system can permit the accessibility all the 2h sessions. Thus, one may foresee that na may first improve with r, and may diminish later [8]. We set r = 10%; 20%; …... 90%, and pick the spot in a unique approach to style an irrelevant “designation design” for various partners. For every blend of r and h, we haphazardly create 104 distinct blends of sessions to be allotted, and the outcomes key set estimating Na is the run of the mill over selective assignments.

6. Experimental Setup

Our systems permit the weight angle (F = n in our plans) to be a tunable parameters, at the cost of O(n) - estimated program parameters. Insurance should be possible in consistent time, while unscrambling should be possible in O(jSj) group duplications (or variable consideration on elliptic bends) with 2 coupling capacities, where S is the arrangement of figure content sessions decode capable by the gave all out key and jSj n [11]. As anticipated, key evacuation needs O(jSj) group duplications also, which appears to be unavoidable. Be that as it may, as affirmed by the exploration results, we don't have to set an extremely extraordinary n to have preferred weight over the tree-based system. Watch that group augmentation is a brisk work.

Table 1. Data Processing with Key Structure with Respect to Time Efficiency

Depth of the Key	Time Efficiency
1	0.04985
2	0.05994
3	0.07012
4	0.08172
5	0.09860

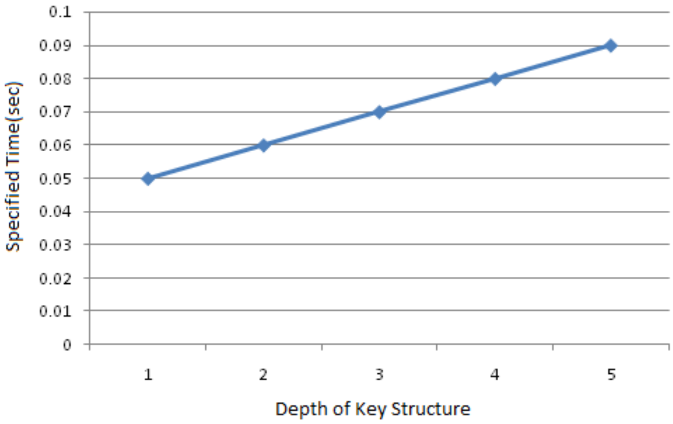

Figure 6. Experiments on Program Installation and Top-Level Sector Power Allow a Setup Operation

Once more, we accept experimentally that our examination is genuine. We connected the essential KAC program in C with the Pairing-Based Cryptography (PBC) Library8 version 0.4.18 for the genuine elliptic-bend group and coupling capacities. Since the gave key can be as meager as one G viewpoint, and the figure message just contains two G and one GT parts, we utilized (symmetric) blends over Type-A (super solitary) shapes as depicted in the PBC accumulation which gives the greatest execution among a wide range of shapes, despite the fact that Type-A shapes don't offer the fastest reflection for group segments.

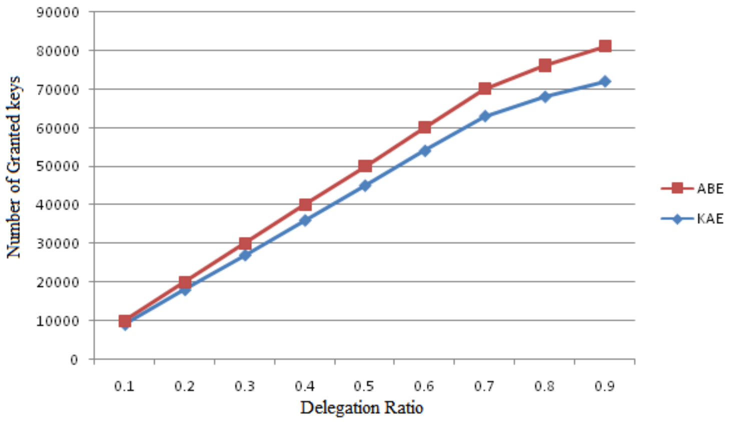

Figure 7. Variety of Provided Important Factors (Na) Needed for Different Approaches in the Situation of 65536 Sessions of Data

The productivity times of Set up, Key Gen, secured are outside of the designation sum r. In our evaluations, Key Gen needs 3:3 milliseconds and Protected needs 6:8 milliseconds. Not surprisingly, the working time issues of Attract out and Decrypt enhance straightly with the designation sum r (which picks the estimating the distributed set S). Our minute results additionally accommodate with what can be seen from the framework in Attract out and Decrypt — two joining highlights take little time, the working length of Decrypt is around a twofold of Attract out. Understand that our evaluations oversaw up to 65536 number of sessions (which is likewise the anxiety figure), and ought to be sufficiently vast for fine-grained subtle elements discussing in many conditions [12]. At long last, we conclusion that for projects where the scope of figure composed content sessions is huge yet the non-private zone for capacity region is restricted, one ought to set up our strategies utilizing the Type-D joining required with the PBC, which just needs 170-piece to speak to a capacity in G. For n = 216, this technique considers needs around 2:6 mb, which is the measure of a lower quality MP3 points of interest PC document or a higher-determination JPEG subtle elements PC record that a typical mobile phone can shop more than various them. In any case, we spared costly ensured range for capacity region without the anxiety of overseeing structure of appointment sessions.

7. Conclusion

In this paper, we show ABE for perceiving versatile, adaptable, and fine-grained accessibility administration in intuition overseeing. arrange effortlessly has a requested structure of framework clients by applying a designation criteria to ABE not just helps material elements because of adaptable arrangement of elements blends, additionally accomplishes productive client end due to a few quality assignments of components. The most effective method to secured clients' points of interest solace is a fundamental inquiry of intuition range for capacity zone. With numerical achievements produced in attribute based encryption for processing data with shared keys in developed application. KAC (Key Aggregate Cryptosystem) performs effective data prediction in terms of data security in real time applications. Our experimental results perform effective data security in outline outsourcing in cloud computing.

References

[1] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in public clouds", IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 9, **(2014)**, pp. 2268-2280.

[2] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model", 2012 IEEE 13th International Conference on Information Reuse and Integration (IRI), **(2012)**, pp. 645-652.

[3] S. Ning, M. Nabeel, F. Paci and E. Bertino, "A privacy-preserving approach to policy-based content dissemination", 2010 IEEE 26th International Conference on Data Engineering (ICDE 2010), **(2010)**, pp. 944-955.

[4] N. Mohamed, E. Bertino, M. Kantarcioglu and B. Thuraisingham, "Towards privacy preserving access control in the cloud", 2011 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), **(2011)**, pp. 172-180.

[5] N. Mohamed, N. Shang, and E. Bertino., "Privacy preserving policy-based content sharing in public clouds", IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 11, **(2013)**, pp. 2602-2614.

[6] N. Mohamed, and E. Bertino, "Poster: towards attribute based group key management", Proceedings of the 18th ACM conference on Computer and communications security, **(2011)**, pp. 821-824.

[7] N. Mohamed, M. Yoosuf, and E. Bertino, "Attribute based group key management", Proceedings of the 14th ACM symposium on Access control models and technologies, **(2014)**.

[8] D. J. Min, Y. J. Song and N. Park, "Attribute based proxy re-encryption for data confidentiality in cloud computing environments", 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI),IEEE, **(2011)**, pp. 248-251.

[9] C. C. Kang, S. S. M. Chow, W. G. Tzeng, J. Zhou and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, **(2014)**, pp. 468-477.

[10] C. S. M. Sherman, Y. J. He, L. C. K. Hui and S. M. Yiu, "Spice–simple privacy- preserving identity-management for cloud environment", International Conference on Applied Cryptography and Network Security, Springer Berlin Heidelberg, **(2012)**, pp. 526-543.

[11] L. Hardesty, "Secure computers aren't so secure", **(2009)**.

[12] W. Cong, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage", IEEE Transactions on computers, vol. 62, no. 2, **(2013)**, pp.362-375.

[13] W. Boyang, S. S. M. Chow, M. Li and H. Li, "Storing shared data on the cloud via security-mediator", 2013 IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), **(2013)**, pp. 124-133.

[14] C. S. M. Sherman, C. K. Chu, X. Huang, J. Zhou and R. H. Deng, "Dynamic secure cloud storage with provenance", Cryptography and Security: From Theory to Applications, Springer Berlin Heidelberg, **(2012)**, pp. 442-464.