IJRSET MAY 2019 Volume 6, Issue 5 Pages: 1-7

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

EFFICIENT ATTRIBUTE BASED MULTIPLE GROUP KEY MANAGEMENT FOR SECURE DOCUMENT ACCESS IN CLOUD SECURITY HEALTHCARE SERVICES

[1] A. ANN USHA MANGALAM,
[1] Assistant professor,
[1] Department of computer Science,
[1] Nirmala college for women, Coimbatore, India.

ABSTRACT: The healthcare services are being moved to the cloud processing condition in the ongoing occasions to make them most effective, interoperate and to team up in the exploration and business areas. In spite of the fact that this will upgrade the services offered by the healthcare providers, the vulnerabilities in the security and execution of the open cloud makes the move less operable. And this paper proposed to multiple group key management scheme to diminish the complexities of the archive clients, get to control grid has been presented through which the capacity intricacy is decreased from 0(n) to 0(3) and calculation complexity can be credited to just a single expansion and two subtraction activities. Correspondingly, if there should be an occurrence of a data proprietor, the quantity of subtraction activities has been diminished from $0(n)^3$ to 0(n) which is the explanation behind decrease in the computational intricacy. Additionally, for the data proprietor, the capacity multifaceted nature acquired is 0(n) as it were. In this way, this work diminishes the overheads caused by both the data proprietors and the cloud clients.

Keywords: [Cloud Data, Healthcare, Key Management, Privacy, Reliability.]

1. INTRODUCTION

A cloud client is an individual (or application following up in the interest of this client) who needs to get to the data from the CSP. At first, each cloud client must send their character credits to the token generator to get a token. The token generator gets the personality qualities from the cloud client and produces a character token. Subsequent to creating this token for a cloud client, in view of their personality qualities, it gives the recently produced character token to the cloud client and after that sends a similar personality token to the data proprietor for check. The confirmation ought to be performed subsequent to giving the token to the cloud client, since the token generator needs to send the character token of a cloud client to the data proprietor just in the event that it is accurately conveyed to that specific cloud client. In the wake of getting affirmation from that cloud client just, the token generator will send the character token to the data proprietor. Every one of these procedures are utilized as clarified in the current methodology. In this work, the current Pedersen duty plot is utilized to protect the privacy of the cloud client to conceal the cloud client's personality from the data proprietor.

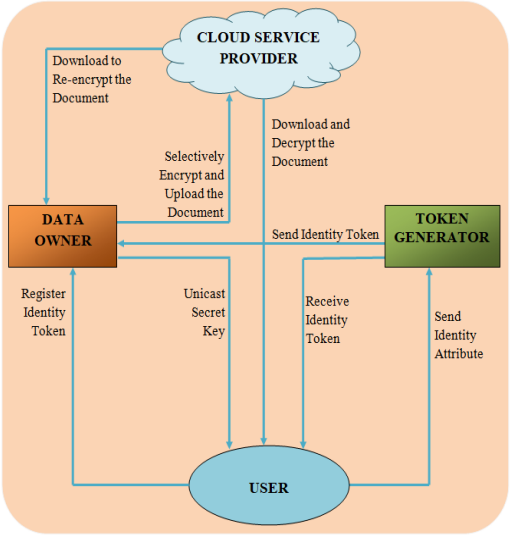

Figure 1: Privacy Preserving Group Key Management Architecture

The framework engineering appeared in Figure 1 comprises of four segments, to be specific, Data Owner, Cloud Service Provider (CSP), Token Generator, and Cloud User. The data proprietor is the person who puts the first archives in the open cloud that are gotten to by the cloud clients. A CSP works a solitary or an accumulation of servers used to keep up the data proprietor's data. The token generator is utilized to create a token which ought to be given to each cloud client to get a mystery key from the data proprietor. The cloud client enlists their character token with the data proprietor to get a mystery key. The data proprietor gives mystery keys to the cloud clients dependent on their personality token. In the wake of giving the cloud client a mystery key, the data proprietor creates a Group Key (GK) for each group of clients. From that point forward, the data proprietor scrambles the group key dependent on their individual mystery key qualities. At that point, the data proprietor communicate the encoded group key in an ACV arrangement to the cloud clients alongside their record esteem. From that point onward, the data proprietor scrambles the subdocuments utilizing group key and after that transfers the encoded subdocuments to the CSP. Each cloud client can determine (recuperate) the GK utilizing their mystery key and in this manner can utilize this GK to unscramble the encoded records put in the cloud. At the point when group enrollment transforms, it is the obligation of the data proprietor to change the GK. The data proprietor may likewise change the GK occasionally. For instance, when a client leaves or joins the group, the data proprietor downloads the comparing archive from the cloud service provider and re-scrambles the record with the new GK. At that point, the re-encoded record is transferred into the cloud. In this work on building up another communicate group key management is concentrated that accepts care of the position of producing the mystery and group keys and furthermore refreshing them when group participation changes. Furthermore, another key recuperation process is additionally acquainted in this work with permit the cloud clients for finding the group key from ACV esteem.

2. LITERATURE SURVEY

Nasarul Islam.K.V, Mohamed Riyas.K.Vproposed dependent on the content documents utilized and the exploratory outcomes it was presumed that DES calculation devours low encryption time and AES calculation has least memory utilization while encryption time distinction is minor in the event of AES calculation and DES calculation, yet RSA Encryption calculations expend a lot of figuring assets, for example, CPU time, memory, and battery control. Correlation of mystery key and open key based DES and RSA calculations, it clears that RSA tackles the issue of the key understanding and key trade issue created covertly key cryptography. In any case, it doesn't tackle all the security foundation.**TalariBhanu Teja,Vootla Hemalatha,K priyanka** proposed Encrypt and Decrypt according to, encoding is the difference in any kind of data into an edge that isn't sensible. Interpreting is the opposition of the scramble which changes over encoded data into reasonable casing. Remembering the

true objective to unravel the encryption, a key which is as often as possible called deciphering key is required for switch tasks. Without a privilege encoded key, a message may not be download. In such conditions, deciphering must be removed from the encryption structures nevertheless, lost the unscrambled key generally result in loss of decoded message.**J. Athena, V. Sumathy**proposed the confinements in the security affirmation and the data privacy restrictions with increment in size of the data on cloud. The advancement of cryptographic methodologies tended to these restrictions and gave the answer for the safeguarding procedure. Due to the multi-occupancy property of the cloud, server and the topographical variables constrained the security of the cloud data access and capacity. **Nallur&Bahsoon**proposed indicates out that due the huge calculation capacity and the transfer speed arrangement in the cloud processing conditions, it is nothing unexpected that the cloud has been a favored stage for some business customers. Since, the QoS offered by the cloud sellers change every now and then and all around profoundly unique in nature, the embodiment of self adaption to the shifting needs to the cloud service dependent on the nature of service is a noteworthy concern. Along these lines, in this examination work, a twofold sale model to enable applications to choose whether a specific assignment can be picked or not is proposed and consequently the customer can browse the numerous merchants. The cloud is the business depiction where the multi-operator applications perform before the customers of the business. This work demonstrates that it is developed contrasted with before works as far as self adaption of single application just as a gathering of uses in general.**Hobfeld et al.**recommended that because of increasingly more business applications lean toward going to cloud, the adaptability and the versatility of the idea of the applications upheld by cloud must be tended to also. However, in actuality, as the organizations will in general move to various cloud stages offered by various merchants with a separated nature of server understanding, the nature of service turns into the real purpose of concern. In addition, the nature of service arrangement by the service providers of the cloud swung out to the rule upon the service providers are characterized for their exhibition. The examination work talks about numerous things about the moving of uses to the cloud and the manner in which the QoS is affected by this moving into the open cloud. Along these lines this novel work by characterizing the cloud applications dependent on the favored nature of service by the clients of the cloud application, gives an examination motivation to the nature of service management.

3. PROPOSED WORK

3.1 Multiple Group Key Management Scheme

We propose another group key management method for different groups known as Multiple Group Key Management Scheme. The single and multi move over a remote system was overseeing for MGKM convention. It will limit rekeying transmission overheads. In this plan, an ace key and numerous slave keys are made from the Master key Encryption calculation. This plan is utilized for giving a group key to the clients. This will decrease the rekeying issue by refreshing the asymmetry of the ace and slave keys. That is one of the slave keys is refreshed, the different keys can be unaltered by changing the ace key. The means to encode and decode data are:

- The records ought to be chosen and transferred into the server.
- Create the group arrangement of endorsers are created and for every supporter inside the bunch a different IP address is made.
- Keys are haphazardly made for each bunch.
- The resultant document will be in scrambled organization.

- To unscramble the record with the assistance of region key and area key ought to be given.

3.1.1 Group Key Computation

The data proprietor produces and scrambles the group key in the accompanying approaches to make the ACV for a specific subdocument and communicate it to the cloud clients of the group.

Theorem 1. The Proposed Key management scheme is correct

Proof: The correction of the proposed scheme can be easily proved as shown below:

$$(\gamma) = (a_{i,1} + \delta_n) - \beta$$
$$(\gamma) = (a_{i,1} + \delta_n - (a_{i,1} + \delta_n - \gamma))$$
$$(Since, (\beta) = (a_{i,1} + \delta_n - \gamma))$$
$$(\gamma) = (a_{i,1} + \delta_n - a_{i,1} - \delta_n + \gamma) = (\gamma)$$

4. EXPERIMENTAL RESULTS

Reliability

Existing 1	Existing 2	Proposed
26	15	41
51	33	89
122	104	137
159	129	176
218	200	233

Table 1: Reliability

The comparison table of Reliability of existing 1, existing 2 and proposed method shows the different values. While comparing the existing method and proposed method the proposed method values are better than the existing method. Existing 1 value starts from 26 to 218 Existing 2 values start from 15 to 200 and the proposed values start from 41 to 233.Every time the proposed method gives the great results.

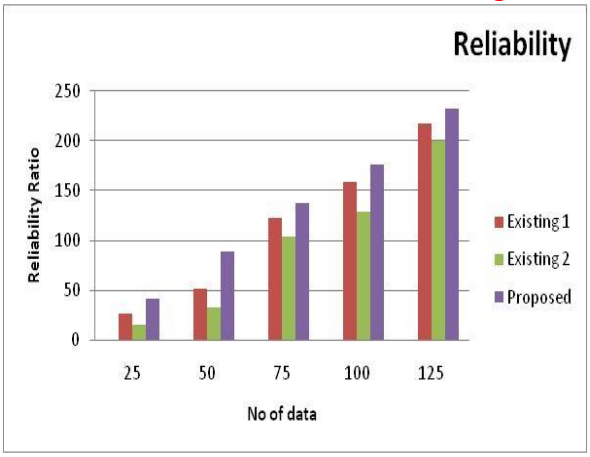

Figure 2: Reliability Chart

The comparison chart of Reliability is demonstrates the existing and proposed method values. No of data in x axis and reliability ratio is y axis. The proposed method values are better than the existing method. Existing 1 value starts from 26 to 218 Existing 2 values start from 15 to 200 and the proposed values start from 41 to 233.Every time the proposed method gives the great results.

Consistency

Existing 1	Existing 2	Proposed
69	47	81
156	142	179
267	233	282
354	329	368
451	430	477

Table 2: Consistency

The comparison table of Consistency of existing 1, existing 2 and proposed method shows the different values. While comparing the existing method and proposed method the proposed method values are better than the existing method. Existing 1 value starts from 69 to 451 Existing 2 values start from 47 to 430 and the proposed values start from 81 to

477.Every time the proposed method gives the great results.

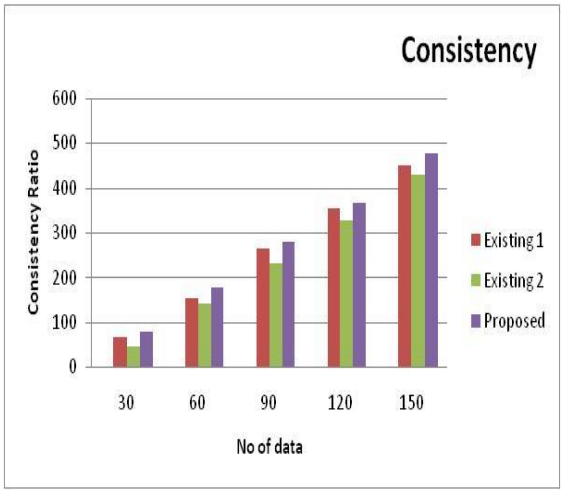

Figure 3: Consistency Chart

The comparison chart of Consistency is demonstrates the existing and proposed method values. No of data in x axis and consistency ratio is y axis. The proposed method values are better than the existing method. Existing 1 value starts from 69 to 451 Existing 2 values start from 47 to 430 and the proposed values start from 81 to 477.

89.Every time the proposed method gives the great results.

Figure 4: Error Reporting

The comparison chart of Error Reporting is demonstrates the existing and proposed method values. No of data in x axis and reporting ratio is y axis. The proposed method values are better than the existing method. Existing 1 value starts from 17 to 99 Existing 2 values start from 22 to 111 and the proposed values start from 9 to 89.

Error Reporting Ratio

Existing 1	Existing 2	Proposed
17	22	9
36	41	25
60	69	47
79	95	62
99	111	89

Table 3: Error Reporting Ration

The comparison table Error Reporting ratio of existing 1, existing 2 and proposed method shows the different values. While comparing the existing method and proposed method the proposed method values are better than the existing method. Existing 1 value starts from 17 to 99 Existing 2 values start from 22 to 111 and the proposed values start from 9 to

Traffic Latency

Existing 1	Existing 2	Proposed
17	26	9
38	49	22
66	81	58
96	113	83
135	140	111

Table 4: Traffic Latency

The comparison table Traffic Latency of existing 1, existing 2 and proposed method shows the different values. While comparing the existing method and proposed method the proposed method values are better than the existing method. Existing 1 value starts from 17 to 135 Existing 2 values start from 26 to 140 and the proposed values start from 9 to

111.Every time the proposed method gives the great results.

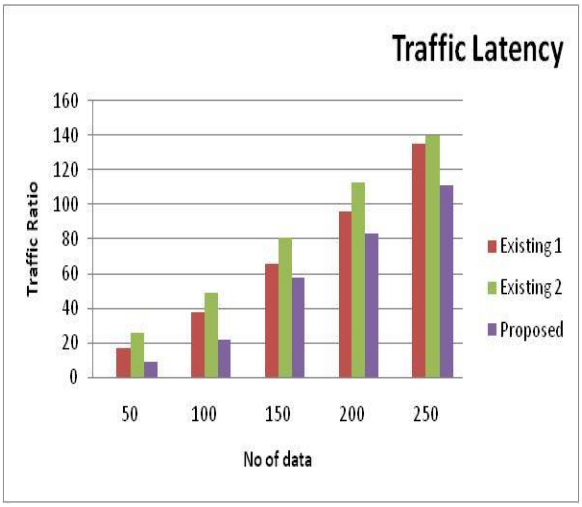

Figure 5: Traffic Latency

The comparison chart of Traffic Latency is demonstrates the existing and proposed method values. No of data in x axis and traffic ratio is y axis. The proposed method values are better than the existing method. Existing 1 value starts from 17 to 135 Existing 2 values start from 26 to 140 and the proposed values start from 9 to 111.

CONCLUSION

The proposed plan has two dimensional centers, to be specific insignificant calculation multifaceted nature and negligible stockpiling intricacy. The calculation unpredictability of the data proprietor is 0(n) and cloud clients computational multifaceted nature is 0(3). As for the correspondence multifaceted nature, the correspondence unpredictability of the proposed plan is 0(1) which implies that the proposed plan takes just a single communicate message as that of Mohamed et al's. plan to advise the ACV incentive to the cloud clients for finding the group key. The capacity unpredictability of data proprietor is 0(n) and the cloud clients stockpiling multifaceted nature is 0(2). The further expansion of this work is to devise a system to deal with record covering.

REFERENCES

[1]. Abdelmaboud, A, Jawawi, DN, Ghani, I, Elsafi, A & Kitchenham, B 2015 'Quality of service approaches in cloud computing: A systematic mapping study', Journal of Systems and Software, vol. 101, pp. 159-179.

[2]. Alkhanak, EN, Lee, SP, Rezaei, R & Parizi, RM 2016, 'Cost optimization approaches for scientific workflow scheduling in cloud and grid computing: A review, classifications, and open issues', Journal of Systems and Software, vol. 113, pp. 1-26.

[3]. Alrokayan, M & Buyya, R 2013, 'A Web portal for management of Aneka based MultiCloud environments', Proceedings of the Eleventh Australasian Symposium on Parallel and Distributed Computing, pp. 49-56.

[4]. Ateniese, G, Fu, K, Green, M & Hohenberger, S 2006, 'Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage', ACM Trans. Information System Security, vol. 9, no. 1, pp. 1-30.

[5]. Audithan, S, Murunya, TS, & Vijayakumar, P 2016, 'Anonymous Authentication for Secure Mobile Agent Based Internet Business', Circuits and Systems, vol. 7, no. 8, pp. 1421-1429.

[6]. Banerjee, S, Gupta, N & Gupta, V 2014, 'Implementation and Management of framework for PaaS in Cloud Computing', International Journal of Innovations & Advancement in Computer Science, vol. 2(2), pp. 38-49.

[7]. Bardsiri, AK & Hashemi, SM 2014, 'QoS metrics for cloud computing services evaluation', International Journal of Intelligent Systems and Applications (IJISA), vol. 6, no. 12, pp. 27-33.

[8]. Barker, S 2007, 'Action-Status Access Control', Proceedings of the 12th ACM Symposium on Access Control Models and Technologies, pp. 195-204.

[9]. Bertino, E & Ferrari, E 2002, 'Secure and selective dissemination of XML documents', ACM Trans Info and System Security, vol. 5, no. 3, pp. 290–331.

[10]. Bertino, E, Castano, S, Ferrari, E & Mesiti, M 2000, 'Specifying and enforcing access control policies for XML document sources', World Wide Web journal, Springer, vol. 3, no. 3, pp.139–151.
[11]. Bertino, E, Piero, A, Bonatti & Ferrari, E 2001, 'TRBAC: A Temporal Role-Based Access Control Model', ACM Transaction Information and System Security, vol. 4, no. 3, pp. 191-233.
[12]. Bethencourt, J, Sahai, A & Waters, B, 2007, 'Ciphertext-Policy Attribute- Based Encryption', Proc. Of IEEE Symp. Security and Privacy (SP '07), pp. 321-334.