IOP Conference Series: Materials Science and Engineering

PURPOSE-LED PUBLISHING™

Quantitative Sørensen–Dice Indexed Damgård–Jurik Cryptosystem For Secured Data Access Control In Cloud

To cite this article: P Calistabebe and D Akila 2020 *IOP Conf. Ser.: Mater. Sci. Eng.* **993** 012093

Quantitative Sørensen–Dice Indexed Damgård–Jurik Cryptosystem For Secured Data Access Control In Cloud

P. CALISTABEBE[1], D. AKILA[2]

[1]Research Scholar, Department of Computer Science,
Vels Institute of Science & Advanced Studies, Chennai, India. calismail@gmail.com
[2]Associate Professor, School of Computing Sciences,
Vels Institute of Science & Advanced Studies, Chennai, India. akiindia@yahoo.com

[1]**Email:** *calismail@gmail.com*
[2]**Email:** *akiindia@yahoo.com*

Abstract Data Access Control has become a demanding issue in cloud storage systems. Access control is the protection method to control who can view or access the information in computing scenarios. Some techniques have been designed formost of the security strategiesprovidedtotheclients accessingtheuploadeddata. AQuantitative Sørensen–Dice Indexing Damgård–Jurik Cryptosystem based Data Access Control (QSDIDJC-DAC) method is introduced to avoid the illegitimate data access in the cloud server. Initially, the QSDIDJC-DAC method comprises five processes, namely registration, key generation, authentication, encryption and decryption for data access. At first, the clientsregister their information to the cloud server. After that, the cloud server generates the key pairs (i.e., public key, private key). Then the client encrypts the data with the general public key and sends it to the cloud server for storing the data. During the data access, the user transmits the request to the cloud server. Upon receiving the request, the authentication server verifies the cloud user is a legitimate user using the Quantitative Sørensen–Dice similarity coefficient with higher authentication accuracy. The Similarity Coefficient matches the requested user with user information stored in the cloud server on the time of registration. Based on the similarity value, the legitimate and illegitimate users are correctly identified with minimum time consumption. After performing the verification process, the cloud server allows legitimate users to access the data. Subsequently, the client decrypts the data with the help of their private key. This helps to enhance the data access control in the cloud server with a better security level. Experimental assessment is carried out on factors such as authentication accuracy, computation time and data confidentiality rate with recognize to some of the cloud users and thedata.

Keywords: cloud computing, access control,Damgård–Jurik cryptosystem, encryption, Quantitative Sørensen–Dice based authentication,decryption

1.Introduction

In current days, the speedy growth of cloud computing has received great attention since the large number of users stores their data on a cloud server. The data's in the cloud server are not below the user's physical control and the unauthorized users easily access the information contained in the server. This leads to a lack of privacy disclosure of the users. To ensure security and confidentiality, the users encrypt their data after which save the data in the structure of ciphertext. But, it is hard for users to explore a huge quantity of ciphertext files. To tackle this issue, efficient cryptosystem has been introduced. An accountable privacy-preserving attribute-based method, known as Ins- PAbAC was introduced in [1] for secure data distribution through the public cloud servers. The designed approach provides the secured access control policies but it failed to achieve a reasonable computation time. An attribute-based controlled collaborative access control scheme was developed [2] for efficiently increases the data confidentiality. However, the scheme was not efficient for providing access control when the multiple data accessed by several users.

A secure and cost-effective attribute-based data access control method has been introduced [3] for cloud storage systems. The designed method was not efficient to provide a higher confidentiality rate. An Identity-Based Signcryption (IBSC) method was designed in [4] for secured data access. The designed method failed to use the efficient encryption method for achieving fine-grained access control. Attribute-based access control with an authorized search method was developed in [5]. The user authentication remained unsolved for achieving the higher security for cloud data access. The Ciphertext-Policy Attribute-Based Encryption (CP-ABE) method was introduced in [6] for data access control. The designed method was not efficient to improve the confidentiality of the data. An incentive method was introduced in [7] for fair data access control. The method minimizes the computation cost but the accurate user authentication was not performed.

Public Key Encryption with Keyword Search (PEKS) was introduced in [8] for access control with multiple users. But the scheme failed for obtaining better performance and security. A Role-Based Access Control (RBAC) model was developed in [9] to address the security problems of cloud storage. Though the method minimizes the time consumption, the authentication was not performed to achieve higher security on data access. An attribute-based access control method has been developed with efficient decryption [10] to considerably minimize the time for data decryption. The method failed to use an efficient cryptographic technique for guaranteeing security. In [11], and efficient NTRU Cryptosystem was introduced to ensure secure and provable access control. The designed Cryptosystem finds legitimate or illegitimate users but it takes more time.

A multiuser access control method has been developed [12] to cloud storage. Though this method minimizes the computation time, the performance validation of data confidentiality prevailed unaddressed. The encryption scheme uses Categorical Quantum Mechanics (CQM) was presented in [13] to solve the access control issue of the cloud. But the performance of various security metrics validation was not performed. An Attribute-Based Signcryption (ABSC) method was introduced in [14] to achieve secure access control. The designed method failed to use more efficient attribute-based encryption to ensure security. A risk-based access control method has been introduced [15] to enhance its security requirements. Thisapproach did not use any cryptographic method for enhancing security for data access.

A trust-based access control approachhas been developed [16] for using fuzzy logic to find authorized or unauthorized users. However, the approach failed to establish mutual access control depends on the trust for increasing the security of data access. A new privacy-aware access control model was developed in [17] to guarantee privacy. The designed model minimizes the computation time but confidentiality was not increased. A Proxy re-encryption based Multi-factor Access Control (PMAC) scheme was developed [18]. Through this scheme performs encryption and decryption, the authentication was not performed. A privacy-preserving mechanism was designed in [19] using hidden access policy toshare data in a public cloud. This mechanism did not minimize the space complexity of storing the ciphertext formation in the attribute-based encryption. A Physical Access Control System (PACS) was introduced in [20] for controlling unauthorized users. But the performance of data analytics capability on a public cloud was not solved.

The issues of the existing literature are resolved by developing a novel QSDIDJC-DAC method. Our main contribution of the QSDIDJC-DAC method as follows,

- A secure access control method called QSDIDJC-DAC is proposed, which employs Damgård–Jurik Cryptosystem and quantitative Sørensen–Dice index-based authentication.
- A quantitative Sørensen–Dice index-based authentication method is applied to find the legitimate or illegitimate users for providing the data access. This helps to improve authentication accuracy and minimizes the computation time.
- The Damgård–Jurik cryptosystem is employed to perform the data encryption and decryption to ensure data confidentiality by providing the data access to legitimate users and declined the access of illegitimate users.
- The implementation of the proposed QSDIDJC-DAC approach has been evaluated and the results show that the authentication accuracy of the proposed method is higher than other baseline approaches.

This paper is arranged into the different sections as given.Section 2 describes the processes of the proposed QSDIDJC-DAC approach with an architecture diagram. Section 3 experimentally verifies its efficacy of the proposed method and existing methods using the dataset. Section 4 discusses the proposed QSDIDJC-DAC Method and compares it to other prediction models. Finally, the conclusion section is presented followed by which the references are cited.

2.Quantitative Sørensen–Dice Indexing Damgård–Jurik Cryptosystem based Data Access Control in cloud

The QSDIDJC-DAC method is introduced to secure data access on the cloud storage. The method mainly consists of five phases such as user registration, key generation, encryption, authentication, and decryption[24]. Key generation process and an authentication process are carried out by the cloud server. The other processes namely user registration and encryption and decryption are performed by the cloud users. The flow diagram of the QSDIDJC-DAC Method is shown in figure 1.

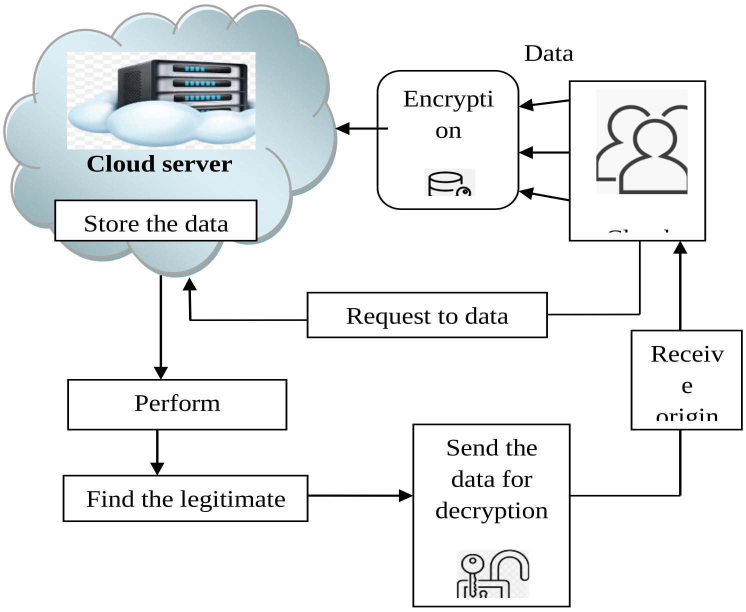

Figure 1 Architecture diagram of the QSDIDJC-DAC Method

As given in Figure 1, the cloud storage system and the system model of QSDIDJC-DAC are given as follows. The cloud architecture consists of three types of entities contributing the secured data access. The entities are cloud server (C_r), authentication server (A_r) and number of cloud users $uc_1, uc_2, uc_3, \ldots. uc_n$. To start with, cloud users perform the registration to store their details to the cloud server for further processing. Followed by which the cloud server produces the keys for each enrolled client. Then the cloud user performs the encryption and stores their data into the cloud server database. At whatever point the client needs to get to the information from the server, the authentication server initially performs the verification to identify the legitimate or illegitimate entity. Finally, the server grants access to legitimate users and denied access to illegitimate users. With the help of these processes, then secured access control is accomplished in a cloud environment[25].

2.1 **Registration & key pair generation**

The registration is the primary phase of the QSDIDJC-DAC method. In this phase, the users registering their appropriate identification details to the server for accessing the various services from the cloud. The users enter their details like name, date of birth, mail ID and so on. These details are sent and stored in the cloud server.

$$uc \xrightarrow{D_t} C_r \quad (1)$$

Where uc denotes a cloud user, D_t indicates the user details, C_r denotes a cloud server. Once the registration is successfully done, the server distributes the pair of keys for all registered users. The cloud server produces the key pair (i.e. private and public key).

$$C_r \rightarrow (k_r, k_b) \ (2)$$

Where, k_r denotes a private key, k_b indicates the public key. The public key is the user ID and the private key of the user is generated using Damgård–Jurik cryptographic algorithm.

Let us select the two random prime numbers u, v and separately of each other.

$$\rho = lcm\ (u-1, v-1)(3)$$

Therefore, the private key (k_r) is obtained as follows,

$$k_r = r \quad (mod\ \rho)\ (4)$$

Where ‘r’ is any positive integer. The generated key pairs (k_r, k_b) are distributed to the registered users as shown in the below figure 2.

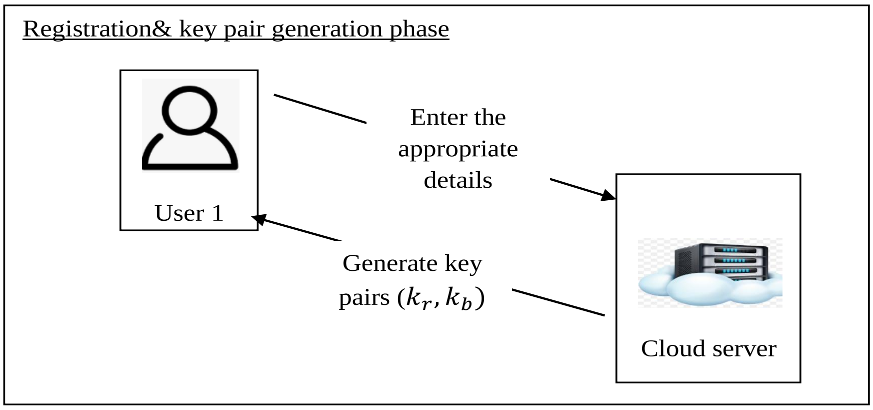
Registration& key pair generation phase
User 1
Enter the appropriate details
Cloud server
Generate key pairs (k_r, k_b)

Figure 2 registration and Damgård–Jurik cryptographic algorithmbased key pair distribution

Figure 2 illustrates the registration and the key pair sharing from the server to the registered users. Upon sharing the pair of keys, the cloud server provides access to the user for secure cloud storage.

2.2 Damgård–Jurik cryptographic encryption algorithm

This phase is invoked when the user stores their data to a cloud server. Because of the increasing idea of cloud users day by day, a huge amount of data stored by the service providers is also increasing rapidly. The primary concern occurs in data privacy since the users storing their confidential information and cloud server are taking care of the security measures of user data. To protect the user confidential information, the cloud server usesDamgård–Jurik cryptographic system to perform the encryption. Therefore, Damgård–Jurik cryptographic is an asymmetric algorithm for improving the data confidentiality and security.

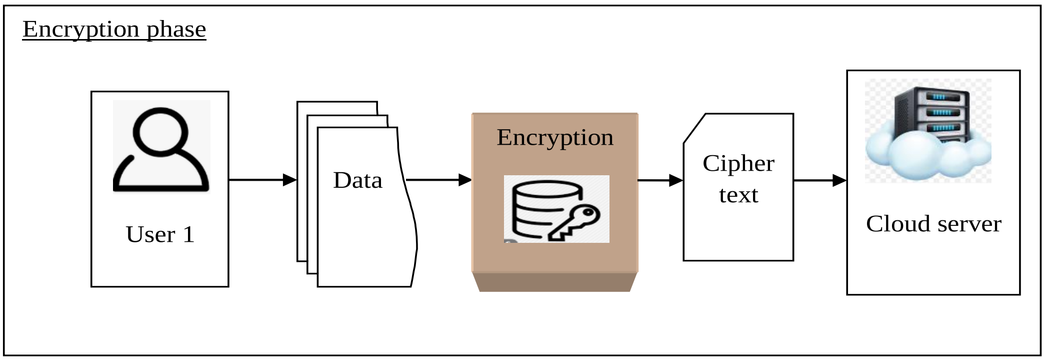

Figure 3 block diagram of Damgård–Jurik cryptographic Encryption

The Damgård–Jurik cryptographic Encryption process to provide the security of user data storage is illustrated in figure 3. At first, Damgård–Jurik cryptographic starts to encrypt each user data with the public key and subsequently, the ciphertext is sent to cloud server for storage.

Let us consider the user data' to be encrypted. The encryption process is carried out as follows,

$$T_c = s^d . p^{z^g} \ mod \ z^{g+1} \quad (5)$$

$$z = u * v(6)$$

$$s = z + 1(7)$$

Where s denotes a random integer, d indicates the data, p refers to the random number, 'z' is the product of the two prime numbers u and v, g denotes an integer number, T_c indicates the ciphertext of original data. The ciphertext is stored in a cloud server for further processing.

2.3 Quantitative Sørensen–Dice index-based authentication

After storing the encrypted data to a cloud server, the authentication is said to be performed whenever the user wants to get the data. The main point of the authentication is to preserve the user data from the access of illegitimate users. This involves that the cloud server rejects the requests from the unknown users and provides the secured access of the confirmed users. In the Quantitative Sørensen–Dice index-based authentication method, the user first sends the demandto access the information by entering the username and password to log in to the system. Then the similarity index matches the requested user with user information stored in a cloud server. Therefore,the similarity is mathematically calculated as follows,

$$\omega = 2 * \left[\frac{I_R \cap I_S}{I_R \cup I_S}\right](8)$$

Where, ω indicates the Quantitative Sørensen–Dice similarity coefficient, I_R represents the user information at login to the system, I_S represents the user information already stored in the server at the time of registration. The symbol '⋂' indicates mutual independence which refers to the information's is independence. The union symbol $' \cup '$ is a mutual dependence which is defined as the two user's information are statistically dependent. The Sørensen–Dice similarity coefficient returns the similarity value somewhere in the range of 0 and 1. If the coefficient returns '1' indicates the user said to be a legitimate user. Something else, the user is said to be illegitimate users. The cloud server provides access to legitimate user and declines the access for the illegitimate users. The flow chart of the authentication is illustrated in figure 4.

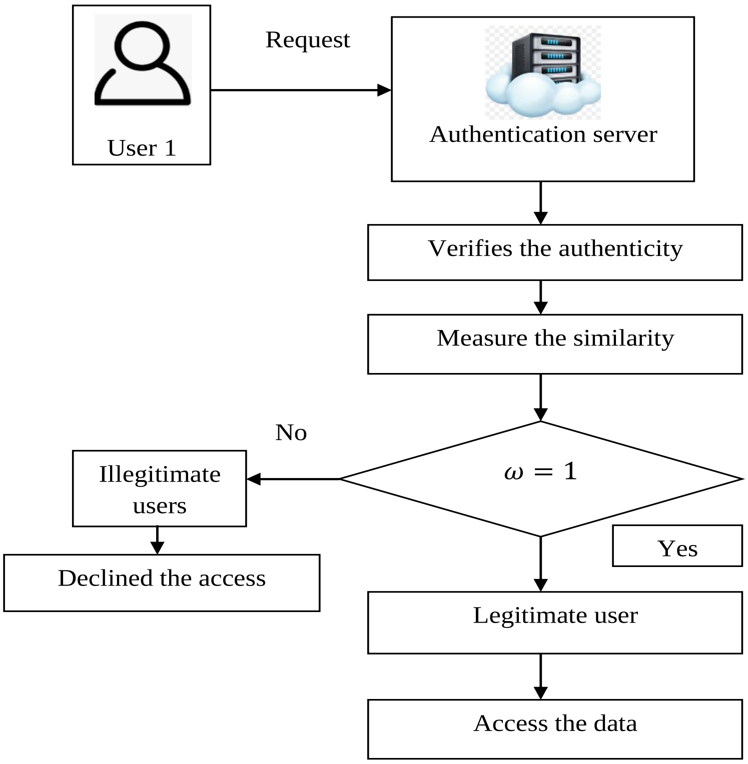

Figure 4 Flow process of Quantitative Sørensen–Dice index-based authentication

Figure 4 describes the flow process of quantitative sørensen–Dice index for user authentication to improve data confidentiality. The user enters the information is verified with the information which is already stored in the cloud server. If both the details are coordinated, at that point the cloud server permits the client to access information. Otherwise, the data access of that user is declined. Therefore, the Quantitative Sørensen–Dice index process improves the authentication accuracy.

2.4 Damgård–Jurik cryptographic decryption algorithm

The final process of the QSDIDJC-DAC method is the decryption to decrypt the ciphertext into the original information. The legitimate user only accesses information from the cloud server to improve secured data access. The flow process of Damgård–Jurik cryptographic decryption algorithm is shown in figure 5.

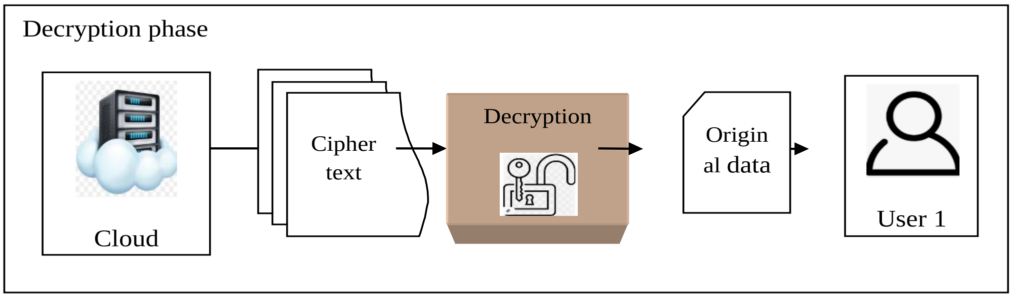

Figure 5 block diagram of Damgård–Jurik cryptographic decryption

The block diagram of Damgård–Jurik cryptographic decryption is illustrated in figure 5. The cloud server provides the user wanted data in the form of ciphertext. The decryption is performed with the help of the user's private key. The decryption process is carried out as follows,

$$d = (nd\ k_r).(nk_r)^{-1}\ mod\ z^g \quad (9)$$

From (9),d indicates the original data of the user, $n\ d$ indicates the relative prime number of data, k_r indicates the private key of a user, $z^g$is a product of two prime numbers u and v, g denotes an integer number. In this way, secured data access is performed in the cloud environment. The step by step process of the QSDIDJC-DAC method is described in algorithm 1. Initially, the registration process is carried out and generates the pair of keys for the users. After that, the input userinformation is encrypted with the public key to obtain ciphertext. An encrypted data stored in the cloud server. If the user wants to access the data, first they verify their authenticity. The authenticity verification is done dependson the similarity measure. Finally, the user is said to legitimate and then the cloud server allows the data access. Then the user decodes the information with their private key and acquires the original information.

Algorithm 1 Damgård–Jurik Dice Similarity Key Matching Cryptosystem based Data Access Control

Input: Number of users $uc_1, uc_2, uc_3, \dots. uc_n$, Number of user data $d_1, d_2, d_3, \dots. d_m$
Output: Improve secure data access

```
Begin
//Registration phase & key pair generation
      For each user '$uc_i$'
         Send their personal information  to cloud server
   $C_r$stores the information into the database
   $C_r$generate a pair of keys $(k_r, k_b)$
   End for
// Encryption
For each user data '$d_i$'
            Encrypt the data $T_c$
            User sends ciphertext into $C_r$
           Store the data into database
End for
 // User authentication
For each user $uc_i$
Checks the authenticity
              Measure the similarity '$\omega$'
If  $(\omega = 1)$ then
                User is said to be a Legitimate user
                Access the data
              else
                User is said to be an illegitimate user
```

```
                    Declined the access
End if
          End for
    // Decryption
         For each Legitimate user
Decryption is performed with a private key ($k_r$)
Get original data 'd'
        End for
End
```

3.Experimental evaluation and parameters description

The experimental evaluations of the proposed QSDIDJC-DAC technique and existing strategies are executed in Java programming Language with a cloudsimulator. To perform the experimental evaluation, the Amazon Access test Dataset is taken from the UCI machine learning storage [21]. Dataset involves the 4 kinds of characteristics namely Person_Attribute, Resource_ID, Group_ID and System_Support_ID that are collected on the cloud server. Giventhe stored information, the cloud server performs authentication and 'remove_access' of illegitimate users or 'add_access of legitimate users[22][23]. In other words, the cloud server provides access to legitimate users'. Otherwise, the cloud server eliminates access to illegitimate users. As a result, the secured access control is performed with the number of cloud clients and the information.

The experimental evaluation is completedwith the different performance metrics are given under,

- ❖ Authentication accuracy
- ❖ Computation time
- ❖ Data confidentiality rate

Authentication accuracy is calculated based on the number of clients in the cloud condition. It is mathematically computed as severalof legitimate clients are effectively-recognized for upgrading the security of information access from the cloud server. The accuracy is estimated as given below,

$$AA = \left\{\frac{Numberofuserscorrectlyidentified}{n}\right\} * 100 \qquad (10)$$

From (10), the authentication accuracy is represented by 'AA', 'n' indicates the number of users considered as input for experimentation. The measurement of authentication accuracy is expressed in terms of percentage (%). In the event, the method has higher accuracy percentage and then the method is said to be better.

The computation time of the algorithm is referred to as the time taken for authentication to ensure security. The authentication time is a measure of time in which the algorithm to identify the legitimate or illegitimate users. The time of the various algorithms is calculated as follows,

$$CT = n * T\ (IOU)(11)$$

Where the computation time of the different algorithms is indicated by 'CT', 'T' is the time taken by identifying the only one user (IOU). The measurement of computation time is in milliseconds (ms).

The data confidentiality rate is a significant performance metric used to guarantee the security of information access. Therefore, confidentiality rate is the quantity of information accessed by legitimate users as well as protected from the illegitimate users from the cloud server. It is calculated as given below,

$$DCR = \left\{\frac{Number of data protected\ from\ ILU}{Total number of data}\right\} * 100 \quad (12)$$

Where, data confidentiality rate is represented by 'DCR', ILU is the illegitimate users. Therefore, the data confidentiality rate is determined in the percentage (%).

4.Performance discussion under different parameters

In this section, the performance results from the experimentation using three methods QSDIDJC-DAC, lns-PAbAC [1],Attribute-based controlled collaborative access control scheme [2] are discussed with various parameters. Initially, the experimental results of authentication accuracy are obtained concerningvarious clients taken as input that counts from 20, 40, 60, 80… 200. The obtained results are shown in Table 1.

Table 1 Authentication accuracy

No. of users	**Authentication accuracy (%)**		
	lns-PAbAC	**Attribute-based controlled collaborative access control scheme**	**QSDIDJC-DAC**
20	85	80	90
40	88	83	93
60	87	82	95
80	88	85	94
100	89	85	92
120	87	83	93
140	89	86	94
160	90	87	93
180	91	88	95
200	89	87	94

The experimental results of authentication accuracy using three different access control methods QSDIDJC-DAC, lns-PAbAC [1],and Attribute-based controlled collaborative access control scheme [2] are shown in table I. The various performance results are obtained for each method. As illustrated in Table I, the accuracy is found to be higher using QSDIDJC-DAC than the conventional methods. By applying the QSDIDJC-DAC method, the authentication is performed using quantitative Sørensen–Dice indexing scheme. Before the data access, the cloud server verifies the authenticity of the client who needs to get to the information. The indexing scheme verifies the user as a legitimate or illegitimate user based on the similarity values. Hence, QSDIDJC-DAC introduces attractive authentication accuracy, especially for cloud data access control.

As shown in table I values, the authentication accuracy of QSDIDJC-DAC is 90% whereas the accuracy of lns-PAbAC [1] and Attribute-based controlled collaborative access control scheme [2] are 85% and 80% respectively with similar input count of 20 users. This shows the QSDIDJC-DAC method outperforms well. The outcomes often results indicate that the average value of authentication accuracy is increased by 6% and 10% than the existing baseline methods [1] [2].

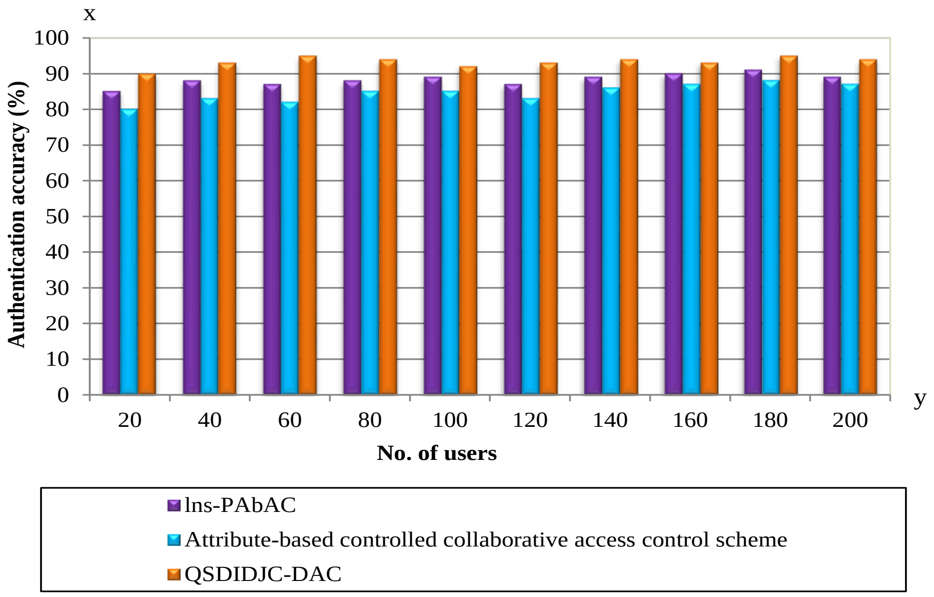

Figure 6Authentication accuracy of proposed and existing methods

Figure 6 illustrates that the authentication accuracy of both proposed QSDIDJC-DAC method and existing of lns-PAbAC [1] and an Attribute-based controlled collaborative access control scheme [2]. The numbers of users are considered as input and the results are obtained at the vertical axis of the graph. The results of various methods are indicated by the different colors to simply identify performance improvement. The above figure 6 notices that the authentication accuracy of the QSDIDJC-DAC method is better than the conventional access control schemes.

The second metric is the computation time used to identify how much time the methods taken for finding legitimate or illegitimate users among the multiple users in the cloud environment. The experimental results of the computation time are illustrated in Table 2.

Table 2 computation time

No. of users	Computation time (ms)		
	lns-PAbAC	Attribute-based controlled collaborative access control scheme	QSDIDJC-DAC
20	18	20	16
40	20	22	18
60	23	25	22
80	27	30	25
100	32	36	29

120	36	40	34
140	39	43	36
160	42	45	40
180	45	47	43
200	48	50	46

Table 2 shows the various performance results of computation time as for the number of clients in the cloud. For the fair comparison of the different methods, there are 10 iterations are performed. The comparisons of the ten resultant outcomes are illustrated in figure 7.

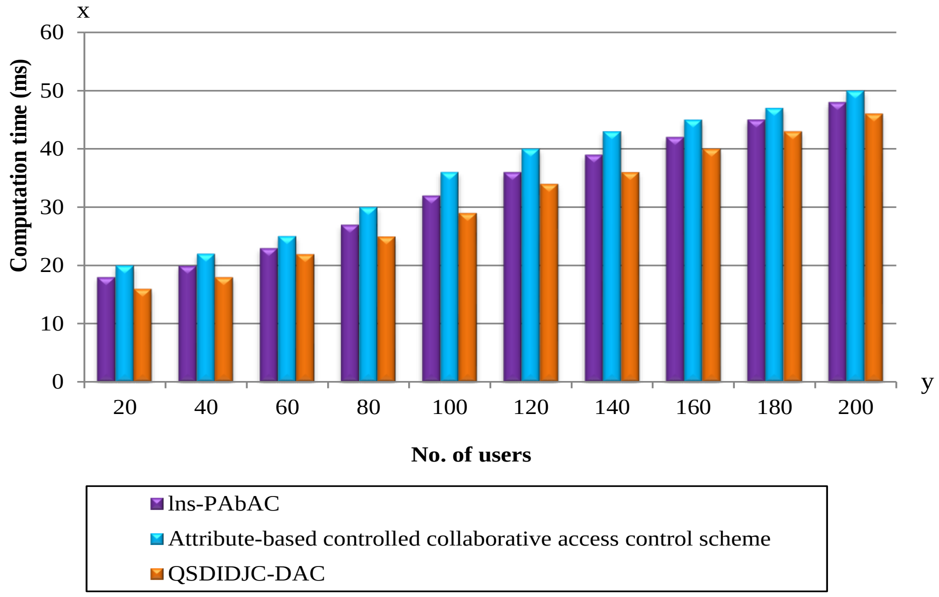

Figure 7 computation time of proposed and existing methods

Figure 7 depicts the computation time of the suggested QSDIDJC-DAC technique and existing of lns-PAbAC [1] along with Attribute-based controlled collaborative access control measure [2]. Above all these computation results, the QSDIDJC-DAC method provides lesser computation time alsogreater security to outsourced data. Meanwhile, increase the number of users, computation time gets expanded. While the computation time of the QSDIDJC-DAC method starts by $16ms$ and increases to 46 ms while requiring 10 runs. But the existing methods have higher computation time. As our accountable QSDIDJC-DAC method relies on the use of storing the user information into the server at the point of the registration phase. Then the similarity measure is performed with the stored information and user-entered details. Therefore, the effects of these operations on the act of the QSDIDJC-DAC method are found to be less. The average of ten results proves that the QSDIDJC-

DAC method achieves lesser computation time for authentication by 7% and 15% than the existing methods.

The final metric is the data confidentiality rate used to enhance the security level of the data access in the cloud. Table 3 and figure 8 gives the experimentation outcome of data confidentiality rate against the quantity of data taken in the counts from 25, 50, 75, ….250.

Table 3 data confidentiality rate

No. of data	Data confidentiality rate (%)		
	lns-PAbAC	**Attribute-based controlled collaborative access control scheme**	**QSDIDJC-DAC**
25	84	80	92
50	80	78	94
75	84	80	91
100	85	82	89
125	84	81	93
150	87	83	95
175	89	85	93
200	88	82	94
225	87	93	93
250	88.4	84	95

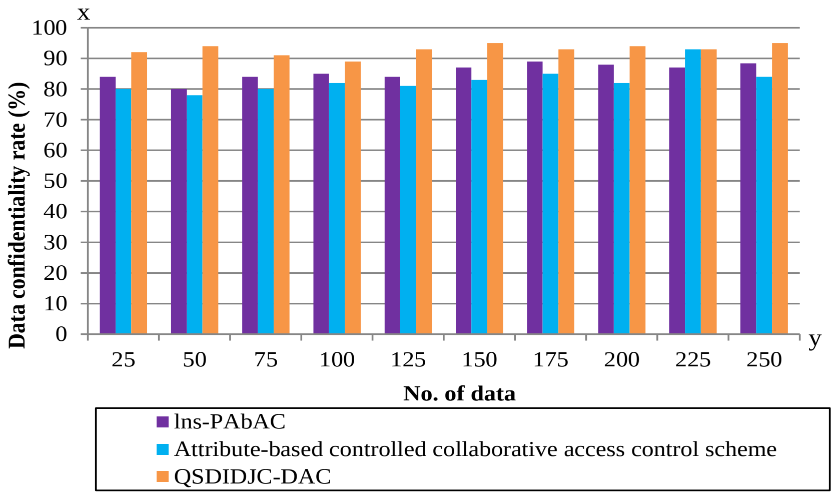

Figure 8 Data confidentiality rate of proposed and existing methods

As depicted by figure 8, the confidentiality rate of three data access control methods with the various number of input data is used. The result indicates that the QSDIDJC-DAC method achieves a higher confidentiality rate than different strategies. This improvement can be achieved by using Damgård–Jurik Cryptosystem. The user pools their information into the cloud server in the form of ciphertext. After that, whenever the user accesses their data, the authenticity is verified first. The legitimate user is identified from the authentication process and the cloud server grants the services to the users and declined the access to the illegitimate users. This process improves the cloud data are only accessed by legitimate users and protected from the other users. Then the legitimate users perform decryption to obtain the original data by converting the ciphertext into plain text. The comparison often results proves that the data confidentiality rate of the QSDIDJC-DAC method is increased by 9% as compared to lns-PAbAC [1] and 12% when compared to Attribute-based controlled collaborative access control scheme [2].

5.Conclusion

This paper presented the QSDIDJC-DAC method that depends on authentication based cryptographic method to safely access the information contents using public cloud servers. The proposed QSDIDJC-DAC method guarantees the confidentiality of outsourced data in public untrusted cloud servers. The QSDIDJC-DAC method also gives adaptable access control approaches among the clients in the cloudenvironment. The Quantitative Sørensen–Dice Indexing based authentication is applied for verifying the user authenticity before the data access. The Damgård–Jurik Cryptosystem is applied to effectively perform data encryption and decryption for effectively supports data confidentiality. The performance of the QSDIDJC-DAC method is very satisfactory. Subsequently,our proposed QSDIDJC-DAC method is exceptionally encouraging to give fine-grained access control with a higher confidentiality rate and authentication accuracy as well as minimizes the computation time.

References

[1]Belguith, S., Kaaniche, N., Laurent, M., Jemai, A., &Attia, R. (2020). Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds. *Journal of Parallel and Distributed Computing*, *135*, 1-20.

[2] Xue, Y., Xue, K., Gai, N., Hong, J., Wei, D. S., & Hong, P. (2019). An attribute-based controlled collaborative access control scheme for public cloud storage. *IEEE Transactions on Information Forensics and Security*, *14*(11), 2927-2942.

[3] Wei, J., Liu, W., & Hu, X. (2016). Secure and efficient attribute-based access control for multiauthority cloud storage. *IEEE Systems Journal*, *12*(2), 1731-1742.

[4] Li, F., Liu, B., & Hong, J. (2017). An efficient signcryption for data access control in cloud computing. *Computing*, *99*(5), 465-479.

[5] Hao, J., Liu, J., Wang, H., Liu, L., Xian, M., &Shen, X. (2019). Efficient Attribute-Based Access Control With Authorized Search in Cloud Storage. *IEEE Access*, *7*, 182772-182783.

[6] Helil, N., &Rahman, K. (2017). CP-ABE access control scheme for sensitive data set constraint with hidden access policy and constraint policy. *Security and Communication Networks*, *2017*.

[7] Liu, H., Li, X., Xu, M., Mo, R., & Ma, J. (2017). A fair data access control towards rational users in cloud storage. *Information Sciences*, *418*, 258-271.

[8] Rao, K. R., Ray, I. G., Asif, W., Nayak, A., &Rajarajan, M. (2019). R-PEKS: RBAC Enabled PEKS for Secure Access of Cloud Data. *IEEE Access*, *7*, 133274-133289.

[9] Xu, J., Yu, Y., Meng, Q., Wu, Q., & Zhou, F. (2020). Role-Based Access Control Model for Cloud Storage Using Identity-Based Cryptosystem. Mobile Networks and Applications, 1-18.

[10] Fu, X., Nie, X., Wu, T., & Li, F. (2018). Large universe attribute based access control with efficient decryption in cloud storage system. Journal of Systems and Software, 135, 157-164.

[11] Hu, C., Li, W., Cheng, X., Yu, J., Wang, S., &Bie, R. (2017). A secure and verifiable access control scheme for big data storage in clouds. IEEE Transactions on Big data, 4(3), 341-355.

[12] Cao, L., Wang, Y., Dong, X., Liu, Y., Zhang, Y., Guo, X., &Feng, T. (2018). Multiuser access control searchable privacy-preserving scheme in cloud storage. International Journal of Communication Systems, 31(9), e3548.

[13] Zhou, L., Wang, Q., Sun, X., Kulicki, P., & Castiglione, A. (2018). Quantum technique for access control in cloud computing II: Encryption and key distribution. Journal of Network and Computer Applications, 103, 178-184.

[14] Srividhya K , Mohan A, Tholkapiyan M, Arunraj A, “Earth Quake Mitigation (EQDM) Through Engineering Design”, Materials Today : Proceedings, ISSN:1904-4720 , Volume 22, 1074-1077, 2020.

[15] dos Santos, D. R., Marinho, R., Schmitt, G. R., Westphall, C. M., &Westphall, C. B. (2016). A framework and risk assessment approaches for risk-based access control in the cloud. Journal of Network and Computer Applications, 74, 86-97.

[16] Kesarwani, A., &Khilar, P. M. (2019). Development of trust based access control models using fuzzy logic in cloud computing. Journal of King Saud University-Computer and Information Sciences.

[17] Lin, L., Liu, T. T., Li, S., Magurawalage, C. M. S., &Tu, S. S. (2017). Priguarder: A privacy-aware access control approach based on attribute fuzzy grouping in cloud environments. IEEE Access, 6, 1882-1893.

[18] Su, M., Wang, L., Fu, A., & Yu, Y. (2018). Proxy Re-Encryption Based Multi-Factor Access Control for Ciphertext in Cloud. Journal of Shanghai Jiaotong University (Science), 23(5), 666-670.

[19] A. Mohan , V.Saravana Karthika , J. Ajith , Lenin dhal , M. Tholkapiyan , “Investigation on ultra high strength slurry infiltrated multiscale fibre reinforced concrete”, Materials Today : Proceedings, ISSN: 1904-4720 , Volume 22, 904-911, 2020.

[20] Petrakis, E. G., Sotiriadis, S., Soultanopoulos, T., Renta, P. T., Buyya, R., &Bessis, N. (2018). Internet of Things.

[21] Dhayachandhran K S, Jothilakshmi M, Tholkapiyan M, Mohan A, “Performance Evaluation and R-Value for Thermally Insulated Wall With Embedding Fluted Sheets”, Materials Today : Proceedings, ISSN: 1904-4720 , Volume 22, 912-919, 2020.

[22] Bebe, P. C., &Akila, D. (2020). An Investigation Study on Secured Data Storage and Access Control in Cloud Environment. In Intelligent Computing and Innovation on Data Science (pp. 223-229). Springer, Singapore.

[23] Bebe, P. C., &Akila, D. (2019, December). Orchini Similarity User Authentication Based Streebog Hash Function for Secured Data Storage in Cloud. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 461-466).IEEE.

[24]Nathiya, T., &Suseendran, G. (2019). An Effective Hybrid Intrusion Detection System for Use in Security Monitoring in the Virtual Network Layer of Cloud Computing Technology.In Data Management, Analytics and Innovation (pp. 483-497).Springer, Singapore.

[25] Mahalakshmi, B., &Suseendran, G. (2019). An Analysis of Cloud Computing Issues on Data Integrity, Privacy and Its Current Solutions.In Data Management, Analytics and Innovation (pp. 467-482).Springer, Singapore.