Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue 5, June 2021: 1257– 1271

Research Article

Tversky Anonymous Key Authentication Based Blum Goldwasser Cryptography For Cloud Data Access Security

K.Mohana Prabha[1], P.Vidhya Saraswathi[2], S.Balamurali[1]

ABSTRACT

Cloud computing is an advanced technology for secured access with available resources. One of the fundamental security needs of data sharing is to guarantee the cloud server could fully control access to an unauthorized entity. In cloud, achieving flexible access of data and protecting privacy of receivers remains challenging issues. To deal with these challenges, a novel technique called Tversky Anonymous Key Authentication based Pseudo Randomized Blum Goldwasser Cryptographic Secured Data Access technique is introduced. The proposed Secured Data Storage technique includes five different steps such as the Registration phase, Anonymous key generation, Authentication, Encryption, and Decryption. Outcomes of Tversky Anonymous Key Authentication based Pseudo Randomized Blum Goldwasser Cryptographic Secured Data Access technique achieves greater secured data access in cloud than the conventional methods.

Keywords: Secure access control, Tversky similarity index based authentication, pseudo-randomized Blum Goldwasser Cryptosystem,

1. INTRODUCTION

Cloud computing is a novel information technology and also satisfies end-users requirements. Security is one of the most demanding issues in cloud with swift improvement of data sources. Many works are already covered a lot about various facets of cloud security. In this paper a solution for resolving issues such as secure access control and authentication over Cloud. In [1] An accountable privacy-preserving attribute-based approach (Ins-PAbAC) was designed for ensuring the privacy of outsourced data.

[1]Department of Computer Applications, Kalasalingam Academy of Research and Education,
Anand Nagar, Krishnankoil-626126. Tamil Nadu,India.
Mail Id:sbmurali@gmail.com Mail Id:kmohanaprabha@gmail.com
[2]Department of Computer Science and Information Technology, Kalasalingam Academy of Research and Education, Anand Nagar, Krishnankoil-626126,
Tamil Nadu,India. Mail Id:vidhyasaraswathi.p@gmail.com

However, designed approach did not use an efficient cryptographic technique to achieve higher confidentiality and integrity. To attain efficient access control in cloud storage, multi-authority ciphertext policy attribute-based encryption (MCP-ABE) technique was presented in [2]. But, it also failed to consider the authentication for enhancing the secure of accessing in the cloud.

In [3] An enhanced attribute-based access control technique was developed for increasing privacy and reliability of data. The technique does not enhance security of data access. In order to distribute data with higher security, Blockchain-based Multi-authority Access Control technique was proposed [4]. But the authenticated access control was not performed. A time and attribute-based dual access control were designed in [5] to increase data integrity. However, the performance of data confidentiality was not achieved at a higher level.

A blockchain-based access control approach was designed in [6] to preserving the privacy of sensitive information. But data integrity was not achieved. In encryption and decryption a secure authentication and data sharing method [7] was developed to minimize the time consumption. To integrate attribute-based access control along with multiple users' Public key encryption with keyword search method [8] was designed.

A privacy-preserving data access control technique has been developed in [9] based on Ciphertext-Policy. The designed method provides higher confidentiality and anonymous authentication. However, the designed method has a higher Authentication Time(AT). To increase confidentiality of client data by avoiding unauthorized access a role-based access control (RBAC) was presented in [10].

Secure elliptic curve cryptography was designed in [11] depend on mutual authentication for improving the privacy of data access. But greater Authentication Accuracy (AA) was not attained. Attribute-based controlled collaborative access control approach [12] was designed for increasing the data confidentiality. However, it failed to consider the authentication process.

With the help of hypergraph construction, attribute-based lightweight access control technique [13] was designed .The designed model attains privacy-oriented confidentiality with the authenticity but the integrity was not considered. A biometric-based authentication was performed in [14] for secured data access. However, an efficient cryptosystem was not applied for enhancing security. An attribute-based access control method [15] was discussed depend on authorized search model. However, accurate authentication was not achieved.

A lightweight anonymous authentication approach was developed in [16] to enhance secured cloud computing services with lesser computation and communication costs [21] – [35]. Elliptic curve cryptography (ECC) was presented in [17] for secured authentication and distribution between the devices. However, the higher data confidentiality and integrity rate were not achieved. To enhance secure access control, A blowfish hybridized weighted attribute-based encryption technique [18] was designed. The technique increases data confidentiality but information-distribution was not performed in a productive manner.

A secured and verifiable access control technique was proposed in [19] to efficiently validate the authenticity of user for accessing the data from cloud. However, an efficient cryptosystem was not applied. A hybrid layered technique was developed in [20] to preserve the data by lattice-based security method. But the designed technique was not efficient for considering the significantly very larger size of records.

The objectives of paper are given,

- To improve secure data access, Tversky Anonymous Key Authentication based Pseudo Randomized Blum Goldwasser Cryptographic Secured Data Access(TAKA-

PRBGCSDA) is introduced based on the Tversky anonymous key authentication and Pseudo Randomized Blum Goldwasser Cryptography.

- To increase the AA with minimum time, Tversky anonymous key authentication is introduced to verify user authenticity before data access. Authorized user gets the input data and guarantees security in cloud.
- A Pseudo Randomized Blum Goldwasser Cryptography is utilized in the TAKA-PRBGCSDA technique to offer ciphertexts of data to authorized users in cloud environment.
- The experiments are performed to estimate TAKA-PRBGCSDA and related works. Results confirm that TAKA-PRBGCSDA is outperformed as compared to state of art work.

The paper is structured as follows –The proposed TAKA-PRBGCSDA with neat architecture is provided in Ssection 2. In Section 3, experimental settings are presented. The implementation results of TAKA-PRBGCSDA and existing methods are discussed in Section 4. At last, the conclusions of the paper are presented in section 5.

2. METHODOLOGY

In distributed cloud environment, secured access control offers data security. Therefore, a conventional access control strategy does not enhance the security level in a distributed environment. In this section, TAKA-PRBGCSDA technique is described with system model, algorithmic definitions, security models, and authentication. Figure 1 illustrates the architecture of the TAKA-PRBGCSDA technique to attain secure access control.

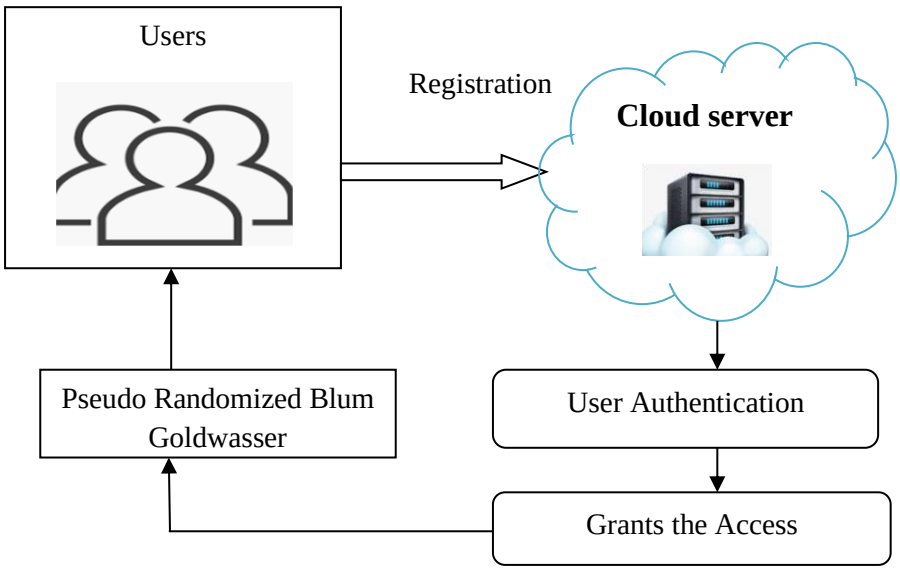

Figure 1. Architecture of the TAKA-PRBGCSDA Technique

2.1 System Model

The problem of secure access control includes dynamic set of different users CU={Cu_1,Cu_2,…..,Cu_n} registers their information to cloud server(CS). CS generates a pair of private and public key K_{pr}, K_{pb} for every registered CU. When cloud user desires to access data from server, authentication server 'A_S' verifies user as authorized or not. When the CU is authorized, the CS grants access otherwise denies access.

2.2 Pseudo randomized Blum Goldwasser Anonymous Key pair generation

Initially users register his/her details such as information's for example Name, DOB, Gender, Contact No, and Mail-ID to CS. Then the CS stores its details of registered user. After the CS sends a properly registered message to users. Then, Anonymous keys (i.e. K_{pr}, K_{pb}) are generated.

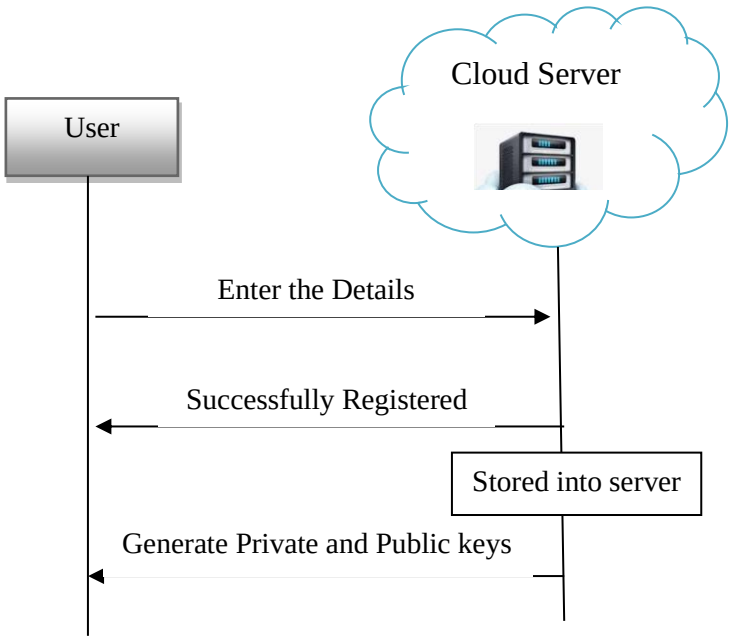

Figure 2. Registration and Anonymous Key Generation

Figure 2 portrays the registration phase and anonymous key generation for secured access control. When the user enters the information, CS gathers details of users and then stored it in the database. For each registered user, the CS generates the private and public keys.

$$Cu_i \xrightarrow{\text{Details}} CS \qquad (1)$$

Where Cu_i indicates the cloud user, CS indicates the cloud server.

$$Cu_i \xleftarrow{\text{SR}} CS \qquad (2)$$

Where SR denotes a successfully registered user. By applying the Pseudo randomized Blum Goldwasser, the private and public keys are generated.

Consider two large prime numbers a and j.

$K_{pb} = m = a * j$ (3)

Where m indicates public key (Kpb),and (a,j) indicates private key (K_{pr}).After generating private and public key, CS distributes the keys to registered users.

2.3 Tversky Similarity Indexed User Authentication

The third process in the TAKA-PRBGCSDA technique is authentication. If user desires to access data, then the server first verifies its authenticity. The authentication server in the cloud verifies the identity of the user by the Tversky Similarity index.

The Tversky index is applied to measure the similarity between private and public keys with already stored keys. A similarity measure is also used to determine the correlation between two variables with a numerical value. Therefore, the Tversky similarity index is evaluated as follows,

$$S = \frac{K_E \cap K_R}{u(K_E \Delta K_R) + v(K_E \cap K_R)} \qquad (4)$$

Where 'S' indicates a Tversky similarity coefficient, K_E signifies the private and public key entered in the login system, K_R indicates the network traffic patterns, $K_E \cap K_R$ denotes a mutual independence between the two keys, $K_E \Delta K_R$ indicates a variance between the keys. In (4), u and v indicate parameters of the Tversky index ($u,v \geq 0$). The similarity coefficient (S) provides the value as 0 or 1. Then the CU is authorized when the both the keys are similar. Otherwise, the CU is identified as not authorized users.

2.4 Pseudo Randomized Blum Goldwasser Encryption

Once the user is authenticated as the authorized user, the CS grants the access. The server offers the user with requested data in encryption form using Pseudo randomized Blum Goldwasser cryptography. The designed cryptography is an asymmetric key encryption algorithm where the K_{pr} is employed for decryption and the K_{pb} is considered for encryption.

Let us consider user requests $UR_i=UR_1,UR_2….UR_n$ and the number of data $D_i=D_1,D_2,….D_n$.The CS encrypts the data and sends into the user in the form of a ciphertext. Let us consider the input data 'D_i' with the public key 'm'. Compute the block size in bits as,

$$H=[\log_2(\log_2 m)] \quad (5)$$

Convert given input 'D' is a sequence of blocks $b_1,b_2,b_3,….,b_r$ with similar bits as

$$Z_0 = R^2 \bmod m \quad (6)$$

Where R denotes a Pseudo random integer R< m For each block 'b_r' computes,

$$Z_i = Z^2_{i-1} \bmod m \quad (7)$$

The ciphertext of the original data is expressed as given below,

$$\varphi_c = b_r \oplus h_i \quad (8)$$

Where, φ_c is a ciphertext, b_r is message block, h_i is least significant bit of Z_i.

$$Z_{r+1} = Z_r^2 \bmod m \quad (9)$$

The encryption of the final message is expressed as given below,

$$E(D) = (\varphi_{c1}, \varphi_{c2},….. \varphi_{cr}, Z_{r+1}) \quad (10)$$

Where, E(D) denotes an encrypted data which is sent to the authorized user with the help of public key 'm'.

2.5 Pseudo Randomized Blum Goldwasser Decryption

Once the authorized user receives the encrypted message, they decrypt ciphertext to original message. Encryption process is performed with user's private key.

$$Z_0 = pwa + qgj \bmod m \quad (11)$$

Where, $p=Z^{d1} \bmod a$, $q=Z^{d2} \bmod j$, *w, g* are pseudo-random numbers, a,j are prime numbers.

$$\text{Where, } d_1 = \left(\frac{a+1}{4}\right)^{r+1} \bmod (a-1) \quad (12)$$

$$d_2 = \left(\frac{j+1}{4}\right)^{r+1} \bmod (j-1) \quad (13)$$

For each block compute,

$$Z_i = Z^2_{i-1} \bmod m \quad (14)$$

The plain text of the ciphertext is expressed as given below,

$$D = \varphi_{ci} \oplus h_i \qquad (15)$$

The decryption of the ciphertext is expressed as given below,

$$W(D) = (b_1, b_2, b_3 \ldots, b_r) \qquad (16)$$

Where, W(D) denotes an original data which is accessed by the authorized user.

This helps to enhance data access security among server and authorized users resulting it increase the data confidentiality and integrity.

// Algorithm 1 Tversky Anonymous Key Authentication based Pseudo Randomized Blum Goldwasser Cryptographic Secured Data Access

Input: Number of users, User requests $UR_i=UR_1,UR_2,\ldots URn$,Cloud Data $D_i=D_1,D_2,,\ldots D_n$
Output: Increase the security of data access

Begin

//Registration and key generation

1. **For every user** Cu_i
2. Enters their details and sent to 'CS'
3. CS sends successfully registered message to the user
4. CS generates 'K_{pr}, K_{pb}'
5. **End for**

// Tversky Similarity Indexed user authentication

6. **for** every registered user
7. CS verifies authenticity
8. **if** (S = +1) then
9. Keys are same
10. The user is said to be an authorized
11. **else**
12. Keys are not same
13. The user is said to be an unauthorized
14. **else if**
15. **end for**

//Pseudo Randomized Blum Goldwasser Encryption

16. **for each** authorized user
17. Cloud server sent the data in the form of encryption 'E(D)**'** with public key 'K_{pb}'
18. **end for**

//Pseudo Randomized Blum Goldwasser Decryption

19. **for each ciphertext**
20. Perform decryption with private key 'K_{pr}'
21. **End for**
22. Obtain the original data 'W(D)'

End

The algorithmic process of the TAKA-PRBGCSDA technique is described with different techniques. At first, each user registers their data into CS for accessing information. Then, the CS simultaneously generates private and public keys to registered user for further processing. Whenever user accesses data from CS, they first need to verify the authenticity. The Tversky

similarity function is used to verify the user entered keys and already stored keys at registration time. Similarity function returns '1' means that both the keys are the same and the user is said to be authorized. Otherwise, the similarity function returns '0'. Therefore, the CS offers the user requested data to authorized users. This helps to improve security in a cloud. The CS delivers the encrypted data to the authorized user with public key of the receiver. After that, user attains original data with private key of receiver. This enhances the Data Confidentiality Rate(DCR).

3. EXPERIMENTAL SETTINGS

Experimental evaluation of TAKA-PRBGCSDA and Ins-PAbAC and MCP-ABE are executed in Java platform .The performances of three methods are carried out by using Amazon EC2 Dataset with CloudSim simulator. For providing the higher security of data access, Amazon EC2 Dataset is applied. The Amazon EC2 Dataset includes divers attributes namely Name, API, storage space, Compute Units (ECU), Cores, Arch, Performance of network, Max Bandwidth (MB/s), Max IPs, Linux cost, and Windows cost. Experimental evaluation using TAKA-PRBGCSDA is carried out with number of cloud users and data.

4. PERFORMANCE ANALYSIS

Experimental results and comparison of TAKA-PRBGCSDA technique and existing Ins-PAbAC [1] and MCP-ABE [2] are discussed with different metrics. The discussion and comparison are performed with tabular and graphical representation. The different parameters are described as given below,

- **Authentication Accuracy** (*AA*): It is defined as ratio of no. of users which are properly authenticated as authorized or not to input no. of cloud users. Therefore, Authentication Accuracy is calculated as follows.

$$AA = \left(\frac{\text{No.of users that are properly identified as authorized or not}}{\text{Input no. of CU}} \right) * 100 \quad (17)$$

- **AT:** It is measured of time consumed to recognize authorized or unauthorized user. AT is measured by,

$$AT = n * \text{time(determine one user as authorized or unauthorized)} \quad (18)$$

Where 'AT' denotes an authentication time, 'n' indicates a number of cloud users. AT is computed in milliseconds (ms).

DCR: It calculated as the ratio of no. of data correctly obtained by authorized user. It is computed in units of percentages (%) and it is calculated as

$$DCR = \left(\frac{\text{No. of data that are correctly obtained by authorized users}}{\text{Total no. of Cloud Data}} \right) * 100 \quad (19)$$

Where 'DCR' denotes data confidentiality

DIR: It is defined as ratio of no. of data received without any modification. DIR is expressed as below,

$$DIR = \left(\frac{\text{No of . received data without any modifications}}{\text{Total number of data}} \right) * 100 \quad (20)$$

Where DIR denotes a Data Integrity Rate is estimated based on dissimilar no. of cloud data.

Tab 1. AA Vs No. of Users

No. of Users	AA (%)		
	TAKA-PRBGCSDA	Ins-PAbAC	MCP-ABE
10	70	60	50
20	70	65	60
30	80	73	70
40	83	75	70
50	82	76	72
60	83	77	73
70	83	76	71
80	84	79	73
90	83	78	73
100	87	82	79

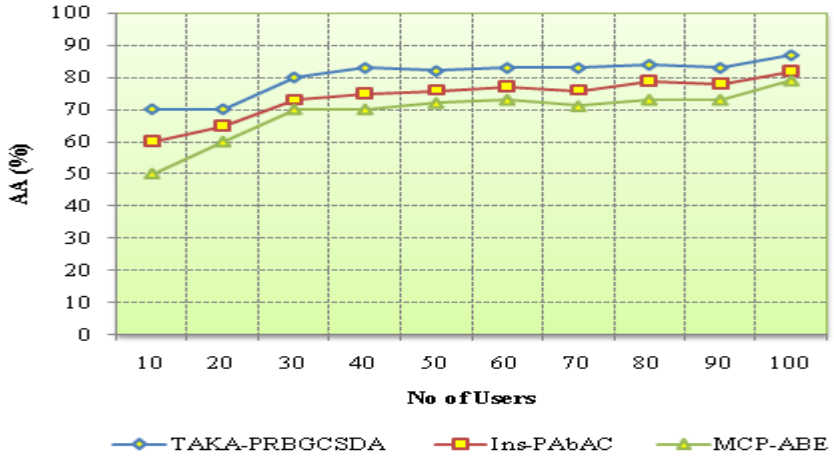

Figure 3. Graphical Illustration of AA

Tab 1 and Figure 3 illustrate the experimental outcome of AA Vs the no of users. As shown in above results, the AA of TAKA-PRBGCSDA is greater than conventional techniques. This enhancement is achieved through Tversky similarity index based authentication technique. If the user desires to access data, then the user enters the system with proper keys. The server uses the similarity function for matching the entered key and stored key at registration time. If these two keys are similar, then the user is authorized. Otherwise, the user is not authorized users. Similarity function in the TAKA-PRBGCSDA technique accurately finds the authorized or unauthorized users. The average of ten results indicates that AA of TAKA-PRBGCSDA technique is enhanced by 9% and 8% than the Ins-PAbAC [1] and MCP-ABE [2] respectively.

Tab 2. AT Versus No of Data

No of Users	AT (ms)		
	TAKA-PRBGCSDA	Ins-PAbAC	MCP-ABE
10	15	16	17
20	26	30	34
30	36	39	42
40	44	48	52
50	48	55	60
60	54	58	66
70	58	63	70
80	62	66	71
90	64	68	73
100	67	70	74

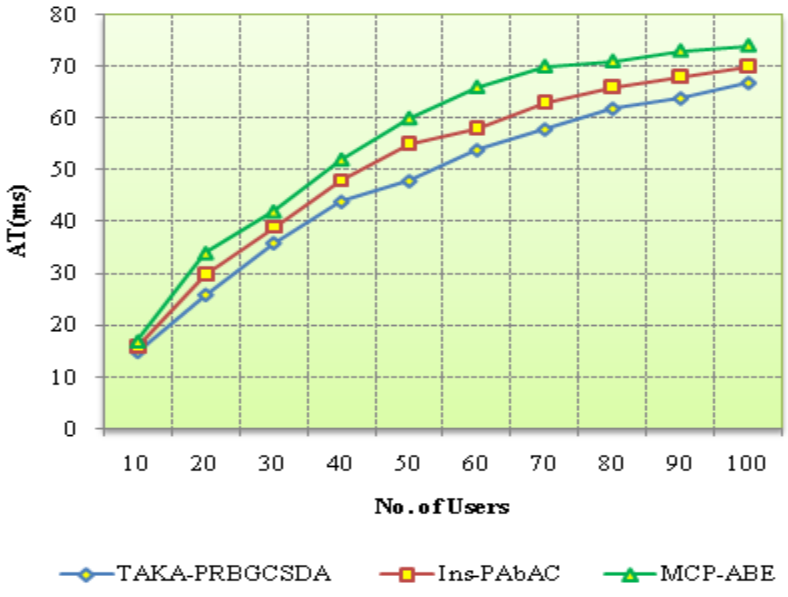

Figure 4. Graphical Illustration of AT

Tab 2 and Figure 4 offer the outcomes of AT with number of users. When increasing counts of users, time consumption for three techniques also increases. This is confirmed through the sample computation, by considering '10' cloud users, the AT of the TAKA-PRBGCSDA technique was found to be '15ms', similarly '16ms' using an Ins-PAbAC [1] and '$17ms$' using [2]. AT for each techniques is obtained and AT is minimized by 9% and 15% than conventional methods. This improvement is achieved by the Tversky similarity index for verifying user authenticity. The similarity function accurately performs the authentication with lesser time.

Tab3. DCR Vs No. of Data

No. of Data	DCR (%)		
	TAKA-PRBGCSDA	Ins-PAbAC	MCP-ABE
25	80	76	72
50	80	78	74
75	85	81	77
100	82	79	75
125	84	81	78
150	85	81	78
175	85	82	78
200	86	83	79
225	86	83	80
250	90	87	84

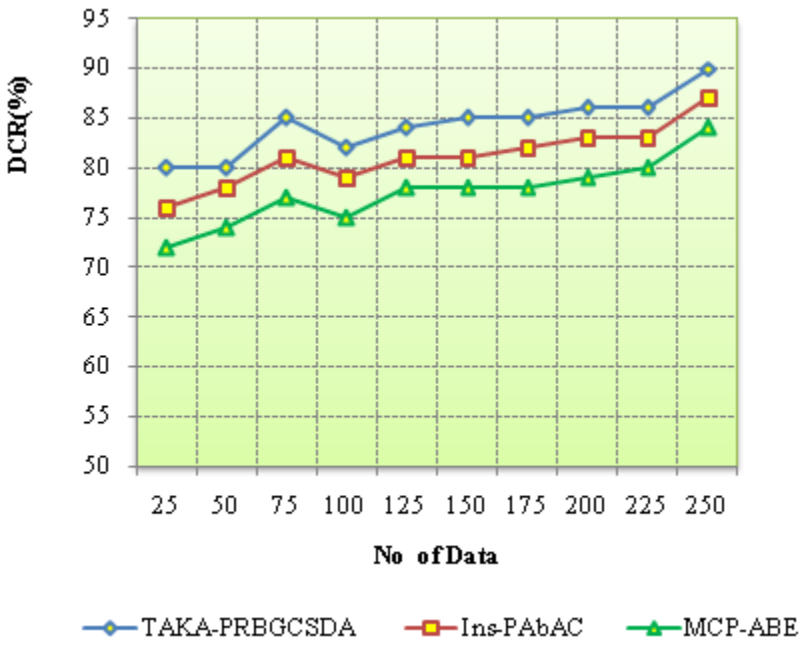

Figure 5. Graphical Illustration of DCR

Table 3 and Figure 5 describe the performance analysis of DCR. A result of TAKA-PRBGCSDA is higher when compared to conventional techniques. This improvement is obtained by applying the authentication as well as encryption. In authentication process, the authorized users are correctly identified and avoid unauthorized users to access data. The Pseudo randomized Blum Goldwasser cryptosystem is also applied for distributing the user requested data in ciphertext form to hide input data. This helps to increase the data confidentiality. The DCR of TAKA-PRBGCSDA technique is improved by 4% and 9% as compared to [1] and [2].

Tab 4. DIR Vs No. of Data

No .of data	DIR (%)		
	TAKA-PRBGCSDA	Ins-PAbAC	MCP-ABE
25	80	72	68
50	82	76	72
75	83	79	75
100	85	80	76
125	86	82	77
150	89	84	80
175	90	85	81
200	91	85	81
225	93	86	82.
250	94	88	85

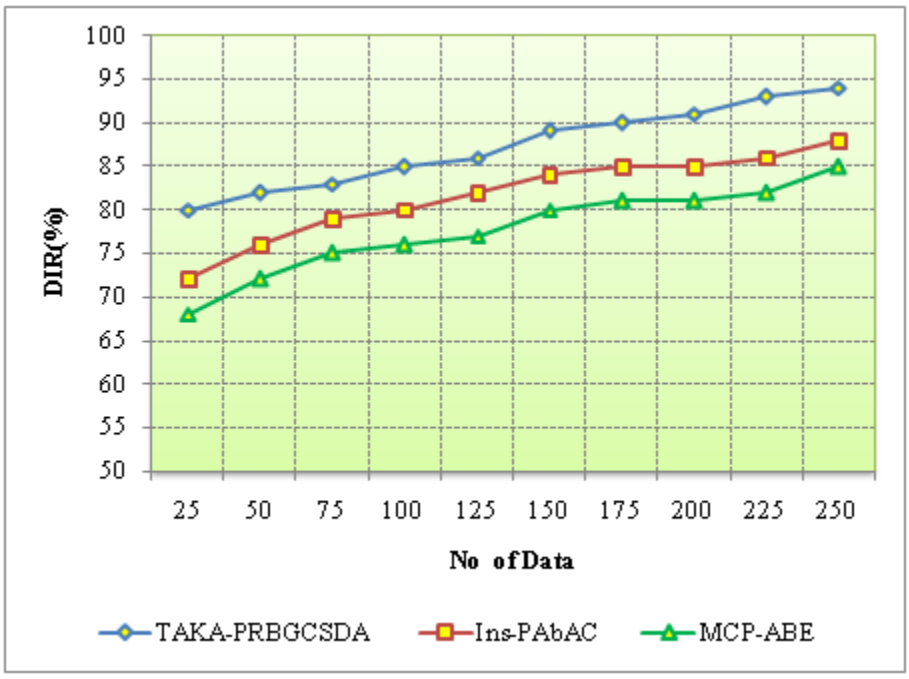

Figure 6. Graphical Illustration of DIR

Tab 4 and Figure 6 reports the performance analysis of DIR with number of data. Observed results illustrate that the input is given to the horizontal axis and the vertical axis represents the data integrity rate. Among the three methods, the TAKA-PRBGCSDA attains greater DIR than conventional techniques. This is proved through the Pseudo randomized Blum Goldwasser cryptosystem provides the user requested data into CS. Authorized user performs data decryption with its private key. Based on data sharing, an authorized person gets the original data. This assists to prevent original data and it did not alter by any intruders. The overall comparison results prove that DIR of TAKA-PRBGCSDA is enhances by 7% and 12% when compared to Ins-PAbAC [1] and MCP-ABE [2] respectively.

5. CONCLUSION

An efficient and secure access control technique called TAKA-PRBGCSDA is introduced. This paper presented an anonymous key generation process after user registration. If user desires to access data, authentication process is performed via Tversky similarity index. Based on authentication, the CS grants services to user. CS response user requested data in ciphertext form by applying pseudo-randomized Blum Goldwasser encryption. Then authorized user decrypts and attains original data. This enhances DCR. The comprehensive experimental evaluation is performed and the outcome specifies TAKA-PRBGCSDA outperformed than the baseline approaches with better DCR, DIR, AA, and lesser AT.

REFERENCES

[1]Sana Belguitha, Nesrine Kaaniche, Maryline, Laurent, Abderrazak JemaiRabah Attia, “Accountable Privacy Preserving Attribute Based Framework For Authenticated Encrypted Access In Clouds”, Journal of Parallel and Distributed Computing,Volume 135, Pages 1-20 January 2020.

[2]Kamalakanta Sethi, Ankit Pradhan, Padmalochan Bera, “Practical Traceable Multi-Authority CP-ABE With Outsourcing Decryption And Access Policy Updation”, Journal of Information Security and Applications, Volume 51, Pages 1-16, 2020.

[3]Praveen Kumar Premkamal, Syam Kumar Pasupuleti, Abhishek Kumar Singh, Alphonse, “Enhanced Attribute Based Access Control With Secure Deduplication For Big Data Storage In The Cloud”, Peer-to-Peer Networking and Applications,Volume 14, Pages 1-19,2020.

[4]Xuanmei Qin, Yongfeng Huang, ZhenYang, Xing, “A Blockchain-Based Access Control Scheme With Multiple Attribute Authorities For Secure Cloud Data Sharing”, Journal of Systems Architecture, volume 112, Pages 1-11,2020.

[5]Qian Zhang, Shangping Wang, Duo Zhang,Jifang Wang, Yaling Zhang, “Time And Attribute Based Dual Access Control And Data Integrity Verifiable Scheme In Cloud Computing Applications”, IEEE Access, Volume 7, Pages 137594 – 137607,2019.

[6]Caixia Yang, Liang Tan ,Na Shi, Bolei Xu,Yang Cao,Keping Yu, “Authprivacychain: A Blockchain-Based Access Control Framework With Privacy Protection In Cloud”, IEEE Access, Volume 8, Pages 70604 – 70615,2020.

[7]Uma Narayanan, Varghese Paul, Shelbi Joseph, “A Novel System Architecture For Secure Authentication And Data Sharing In Cloud Enabled Big Data Environment”, Journal of King Saud University – Computer and Information Sciences, Pages 1-15,2020.

[8]Rajesh Rao, Indranil Ghosh Ra, Waqar Asif, Ashalatha Nayak, Muttukrishnan Rajarajan, "R-PEKS: RBAC Enabled PEKS For Secure Access Of Cloud Data", IEEE Access, Volume 7, Pages 133274 – 133289,2019.
[9]Qian Xu, Chengxiang Tan, Zhijie Fan, Wenye Zhu, Ya Xiao, Fujia Cheng, "Secure Multi-Authority Data Access Control Scheme In Cloud Storage System Based On Attribute-Based Signcryption", IEEE Access,Volume 6,Pages 34051 - 34074,2018.
[10]Jian Xu, Yanbo Yu, Qingyu Meng, Qiyu Wu, Fucai Zhou, "Role-Based Access Control Model For Cloud Storage Using Identity-Based Cryptosystem", Mobile Networks and Applications, Pages 1-18,2020.
[11]Vinod Kumar, Musheer Ahmad, Adesh Kumari, "A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol For Cloud-Assisted TMIS", Telematics and Informatics, Volume 38, Pages 1–21,2019.
[12]Yingjie Xue, Kaiping Xue, Na Gai, Jianan Hong, David S. L. Wei, Peilin Hong, "An Attribute-Based Controlled Collaborative Access Control Scheme For Public Cloud Storage", IEEE Transactions on Information Forensics and Security, Volume 14,Issue 11, 2019, Pages 2927 – 2942.
[13]Mythili, Revathi Venkataraman, Sai Raj, "An Attribute-Based Lightweight Cloud Data Access Control Using Hypergraph Structure", The Journal of Supercomputing,Volume 76, Pages 6040-6064,2020.
[14]Deepnarayan Tiwari, Gayatri K Chaturvedi, Gangadharan, "ACDAS: Authenticated Controlled Data Access And Sharing Scheme for Cloud Storage", International Journal of communication system, Wiley, Volume 32, Issue 15, Pages 1-112019.
[15]Jialu Hao, Jian Liu,Huimei Wang, Lingshuang Liu, Ming Xian, Xuemin Shen, "Efficient Attribute-Based Access Control With Authorized Search In Cloud Storage", IEEE Access, Volume 7, Pages 182772 – 182783,2019.
[16]Hamza Hammami, Sadok Ben Yahia, Mohammad S. Obaidat, "A Lightweight Anonymous Authentication Scheme For Secure Cloud Computing Services", The Journal of Supercomputing, Volume 77, Pages 1-21, 2020.
[17]Saru Kumari, Marimuthu Karuppiah, Ashok Kumar Das, Xiong Li, Fan Wu,Neeraj Kumar, "A Secure Authentication Scheme Based On Elliptic Curve Cryptography For IOT And Cloud Servers", The Journal of Supercomputing,Volume 74, Pages 6428-6453,2018.
[18]Smarajit Ghosh, Vinod Karar, "Blowfish Hybridized Weighted Attribute-Based Encryption For Secure And Efficient Data Collaboration In Cloud Computing", Applied Science, Volume 8, Pages 1-15, 2018.
[19]Chunqiang Hu, Wei Li, Xiuzhen Cheng, Jiguo Yu, Shengling Wang, Rongfang Bie, "A Secure And Verifiable Access Control Scheme For Big Data Storage In Clouds", IEEE Transactions on Big Data, Volume 4, Issue 3, Pages 341 – 355,2018.
[20]Saravanan, Umamakeswari, "Lattice Based Access Control For Protecting User Data In Cloud Environments With Hybrid Security", Computers & Security, Volume 100, Pages 1-22, 2020.
[21] Ramamoorthy, S., Ravikumar, G., Saravana Balaji, Balakrishnan S. et al. MCAMO: multi constraint aware multi-objective resource scheduling optimization technique for cloud infrastructure services. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02138-0.
[22] Ponmagal, R.S., Karthick, S., Dhiyanesh, B, S. Balakrishnan & K. Venkatachalam. Optimized virtual network function provisioning technique for mobile edge cloud computing. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02122-8.

[23] S. Balakrishnan, J. Janet, K.N. Sivabalan, “Secure Data Sharing in a Cloud Environment by Using Biometric Leakage resilient Authenticated Key Exchange”, Pak. J. Biotechnol. Vol. 15 (2) 293-297 (2018).
[24] S. Balakrishnan, D.Deva, “Internal or External - Which Database Could Contribute More to Business Intelligence?” CSI Communications magazine, Vol. 42, issue 7, October 2018, pp. 24-25. ISSN: 0970-647X.
[25] J. Janet, S. Balakrishnan and E. Murali, "Improved data transfer scheduling and optimization as a service in cloud," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-3. doi: 10.1109/ICICES.2016.7518895.
[26] Balakrishnan S., Janet J., Spandana S. ”Extensibility of File Set Over Encoded Cloud Data Through Empowered Fine Grained Multi Keyword Search”. In: Deiva Sundari P., Dash S., Das S., Panigrahi B. (eds) Proceedings of 2nd International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 467. 2017. Springer, Singapore.
[27] J. Janet, S. Balakrishnan and K. Somasekhara, "Fountain code based cloud storage mechanism for optimal file retrieval delay," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-4. doi: 10.1109/ICICES.2016.7518901.
[28] J. Janet, S. Balakrishnan and E. R. Prasad, "Optimizing data movement within cloud environment using efficient compression techniques," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-5. doi: 10.1109/ICICES.2016.7518896.
[29] M. Balasubramaniyan, M. Balasubramanian, S. Balakrishnan, “Data Movement Optimization In A Cloud Environment Using Capacity Optimization Technique”, Jour of Adv Research in Dynamical & Control Systems. Vol. 10, 11-Special Issue, 2018, pp. 740- 743.
[30] Sruthi Anand, N.Susila, S.Balakrishnan, Challenges and Issues in Ensuring Safe Cloud Based Password Management to Enhance Security”, International Journal of Pure and Applied Mathematics, Volume 119, No. 12, 2018, pp.1207-1215.
[31] Dipon Kumar Ghosh , Prithwika Banik , Dr. S. Balakrishnan (2018), “Review-Guppy: A Decision-Making Engine for Ecommerce Products Based on Sentiments of Consumer Reviews”, International Journal of Pure and Applied Mathematics, Volume 119, No. 12, 2018, pp.1135-1141.
[32] K. Aravind, J. Granty Regina Elwin, T. Sujatha and S. Balakrishnan, (2018), “A Novel And Efficient Mobile Cloud Service For Searching Encrypted Data”, ARPN Journal of Engineering and Applied Sciences, Vol.13, No.16, pp. 4683- 4686, 2018.
[33] Suresh Kumar, K., Balakrishnan, S. & Janet, J. A cloud-based prototype for the monitoring and predicting of data in precision agriculture based on internet of everything. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02632-5
[34] Balakrishnan S and Steven Uatuaromuinjo Tjiraso, “Integration of Agent Based Computing with Cloud Computing: Towards Cloud Intelligent Systems”, International Research Publication House, Delhi. Engineering and Technology: Recent Innovations & Research, ISBN- 978-93-86138-06-4, pp. 1-17.
[35] S.Sheeba Rani, S.Balakrishnan, V.Kamatchi Sundari, K.C.Ramya, IoT Based Water Level Monitoring System for Lake in a Cloud Environment, International Journal of Lakes and Rivers (IJLR), Vol. 12, Issue 1, (2019), pp. 21-25.