IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Ensuring Secured Data Sharing in Cloud through Attribute-Based Signcryption Scheme to Improvise Data Confidentiality

V. Reena Catherine[1], A. Shajin Nargunam[2]

Research Scholar in Computer Science, Noorul Islam Centre for Higher Education, Kumaracoil, Tamilnadu, India [1].

Director /Academic Affairs, Noorul Islam Centre for Higher Education, Kumaracoil, Tamilnadu, India [2].

ABSTRACT : Usage of internet and its associated resources has taken a massive exponential growth in recent years. Thus cloud computing has gotten a lot of admirers and a wider range of users. The benefiters are freed from operational and maintenance costs for the used resources. Paying only for the used resources is what exactly needed by every cloud user. But there is always a fear among the users in terms of the security of the confidential data being stored in the cloud. There is no guarantee that impostors may try to steal the data or expose confidential information. In order to overcome this fear, various encryption schemes have been followed over the years. Preserving the secret keys has been a challenge that leads one scheme to another. In this paper a scheme called Ciphertext-Policy Attribute-Based Signcryption with Outsourced Designcryption(CP-ABSc-ODs) is proposed. Also enabling the users to outsource the designcryption process reduces the burden of computation overhead. This also provides option for verifying the designcryption process as the outsourcer cannot be a fully trusted server. The time usage for signcryption, designcryption, key response and partial decryption are analyzed with existing schemes and proven that our scheme is efficient and secure for improvising data confidentiality thus ensuring secured data sharing in the cloud.

KEYWORDS: Attribute-based signcryption, cloud security, data confidentiality, outsourcing.

I. INTRODUCTION

Ubiquitous and edge computing is the latest trend that uses the resources in the efficient way and paying only in a metered way. The pandemic situation has also turned the attention of many people to cloud computing as homes are getting converted into offices and virtual classrooms. Ease of use is the key mantra for cloud users. But the greatest concern is about the security threat to the confidential data being transferred and stored in the cloud. The storage destination is unknown to the user and so there is always the fear of being exposed accidentally or purposefully. E-commerce and money transfer through the internet have become a boon to mankind. Fewer or minimal interaction from service providers [1] has made cloud computing a major player in the technological universe.
Clouds are classified into private, public, community and hybrid based on the usage and ownership. Also clouds are classifies into Infrastructure as a Service, Platform as a Service and Software as a Service based on the provided services.

Moving valuable data to the cloud is always risky as the genuineness of the Cloud Service Provider is not assured. Trust cannot always be built and so every cloud data owner and data user of confidential data is made to follow some strategies to safeguard security to the valuable and secret data. Threat need not be from malicious intruders but even the CSP can be the culprit to expose confidential data. Data remanence and multi tenancy also add to the risks.
While shifting data to the cloud [2], data owners must ensure some policies to ensure data integrity and confidentiality. CSPs also gain power in handling the data. So it becomes essential to prevent CSP from intrusion, giving sole authority to the data owners on deciding what is to be done o their data and letting only privileged users to gain access to the data [3]. To achieve these major points, various cryptographic schemes [4], [5] are used. Encrypting the confidential information on the owner side and then moving into the cloud is followed for security reasons. But it introduces additional computations to get back the original data.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

II. RELATED WORK

Data confidentiality means prevention of any data from illegal access by intruders but permitting only authorized users to access them. It is always advisable to encrypt the data before storing in the cloud as cloud is not fully trustworthy. Many cryptographic schemes have been introduced and used. Traditional encryption schemes used numeric keys but the keys should never be compromised. Only key holders are able to encrypt and decrypt the content. In Identity-Based Encryption unique ids were kept as public keys.

This scheme was improvised into Identity-Based Broadcast Encryption facilitating an encrypted content to be broadcasted to a group of recipients. Later came into the field is Attribute-Based Encryption where the encryption can be done with the help of an access policy and a set of attributes of the authorized users [6,7,8]. Ciphertext-Policy ABE requires encryption to be done using attributes and decryption only if access policy is satisfied. Fully Homomorphic Encryption [9,10] permits computations on the ciphertext itself. Searchable Encryption [11,12,13] allows search operation to be carried out on ciphertext eliminating the need to decrypt. Order Preserving Encryption [14] ensures the preservation of order of ciphertext with its corresponding plaintext. Time Release Encryption [15,16] permits different users to release time sensitive data upon satisfying the time constraints. The concept of Attribute-Based Signatures [17] was introduced for authentication and combined with CP-ABE to give CP-AB Signcryption [18].Partial decryption was outsourced in CP-OABSC scheme [19].

III.PROPOSED METHODOLOGY

The challenges encountered in using cloud storage are:

a) cost of key generation and encryption/decryption is based on the complexity of the access policy and

b) outsourcing decryption can reduce the user's computation load but adds communication cost.

In this paper, an improvised encryption technique entitled Ciphertext-Policy Attribute-Based Signcryption with Outsourced Designcryption is proposed for solving the above said issues. Verification of the designcryption process is made available. Also adding signature provides authenticity and accountability to the scheme making it an advantageous one.

The four major phases of CP-ABSc-ODs protocol are as follows.

System Setup

1. Choose a prime number p with generators g1 for G1 and g2 for G2 with bilinear mapping $e: G_1 \times G_2 \rightarrow G_3$.
2. Randomly choose exponents $\alpha, \beta \in Z_p$.
3. Choose a hash function $H_1 : \{0,1\}^* \rightarrow Z_p$.
4. Calculate $P_k = (p, G_1, G_2, H_1, g_1, g_2, h = g_1^{\beta}, t = e(g_1, g_2)^{\alpha})$ and publish the public components.
5. Calculate the private component MSK=($P_k = (\beta, g_2^{\alpha})$)

Key Generation

Input: Master Secret Key and attribute set S of an entity.

1. Choose randomly $r_{en}, r_{sn \in Z_p}$
2. Compute the private component $Den = g_2 \frac{(\alpha + r_{en})}{\beta}$ and sign key $K_{sign} = g_2 \frac{(\alpha + r_{en})}{\beta}$
3. Foe every attribute $j \in s$ do
4. Choose randomly $r_j \in Z_p$
5. Calculate $D_j = g_2^{ren} . g_2^{(H_1(j).r_j)} and\ D'j = g_2^{rj}$
6. End for
7. Calculate secret key $Sk = (Den, \forall_j \in s : D_j, D'j)$
8. Calculate verification key $Kver = g_2^{rsn}$

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

9. Send Sk and K_{sign} to the entity and publish K_{ver} to others to verify the entity if needed.

Signcryption

Input: Public key, plaintext M, access tree T with root R and signing key K_{sign}.

1. Select a polynomial q_x and set the degree $d_x = k_x - 1$ for every node in T
2. Choose randomly s ∈ Z_p and set $q_R(0) = s$
3. Choose d_R random numbers
4. from Z_p to define polynomial q_R.
5. for any other node x in T do
6. Set $q_x(0) = q_{parent(x)}(index(x))$
7. Select d_x random numbers from Z_p to define q_x.
8. End for
9. Let Y be the set of leaves in T.
10. Construct ciphertext CT based on tree T as: $CT = (T, \tilde{C} = M \oplus t_s, C = h^s, \forall y \in Y : C_y = g1^{qy(0)}, C'_y = g_1^{(H_1(att(y)).q_y(0))})$
11. Choose a random $\xi \in Z_p$ and compute $\delta = e(C, g^2)\xi, \pi = H_1(\delta \mid M), and\ \Psi = g_2\xi.(Ksign)\pi.$
12. Output the message: $CT_{sign} = (T, \tilde{C}, C, \forall y \in y : C_y, C'_y, W = g_1 s, \pi, \psi)$

Designcryption

Input: CT_{sign} = (CT, W, π, ψ);private key SK for designcryption and set of attributes S.

1: A = Decrypt Node(CT, SK, R)

2: if $A \neq \perp$ then

3: $\tilde{A} = e(C, Den) / A$

4: End if

5: Calculate $\delta' = \frac{e(C, \psi)}{(e(W, K_{ver}).\tilde{A}^{\pi}}$

6: if $H_1(\delta' \mid M') = \pi$ then

7: return $M = M'$

8: end if

9: Return ⊥

Figure 1 shows the architecture diagram of the proposed work. A data owner signcrypts and then uploads the personal data to a Cloud Storage Server (CSS) which is a fully trusted one. A data user in need of such data already stored in CSS must satisfy the access policy by the respective attribute sets. On having access permission, the user connects with the semi-trusted ciphertext transformation server (STS) using a session and initiates transformation.

The CTS sends back the required transformed ciphertext. User has the facility to verify the integrity of this transformed ciphertext and then retrieve the desired original text with the help of private and corresponding transformation key. On finding any discrepancy during decryption, the data user can immediately contact the Trusted Attribute Authority legally.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

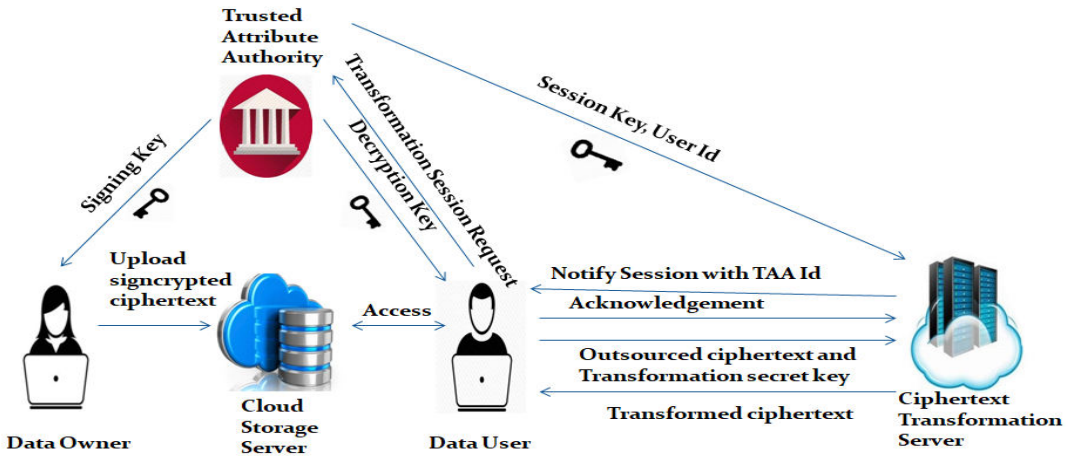

Figure 1: Architectural Diagram of CP-ABSc-ODs)

Figure 2 shows the high-level description of the scheme. The CTS and the user establish a session to perform the designcryption process in a systematic manner. Each session will have a unique session ID. In case of decryption failure, authentication can be checked by the user. Session keys are destroyed automatically to maintain forward secrecy.

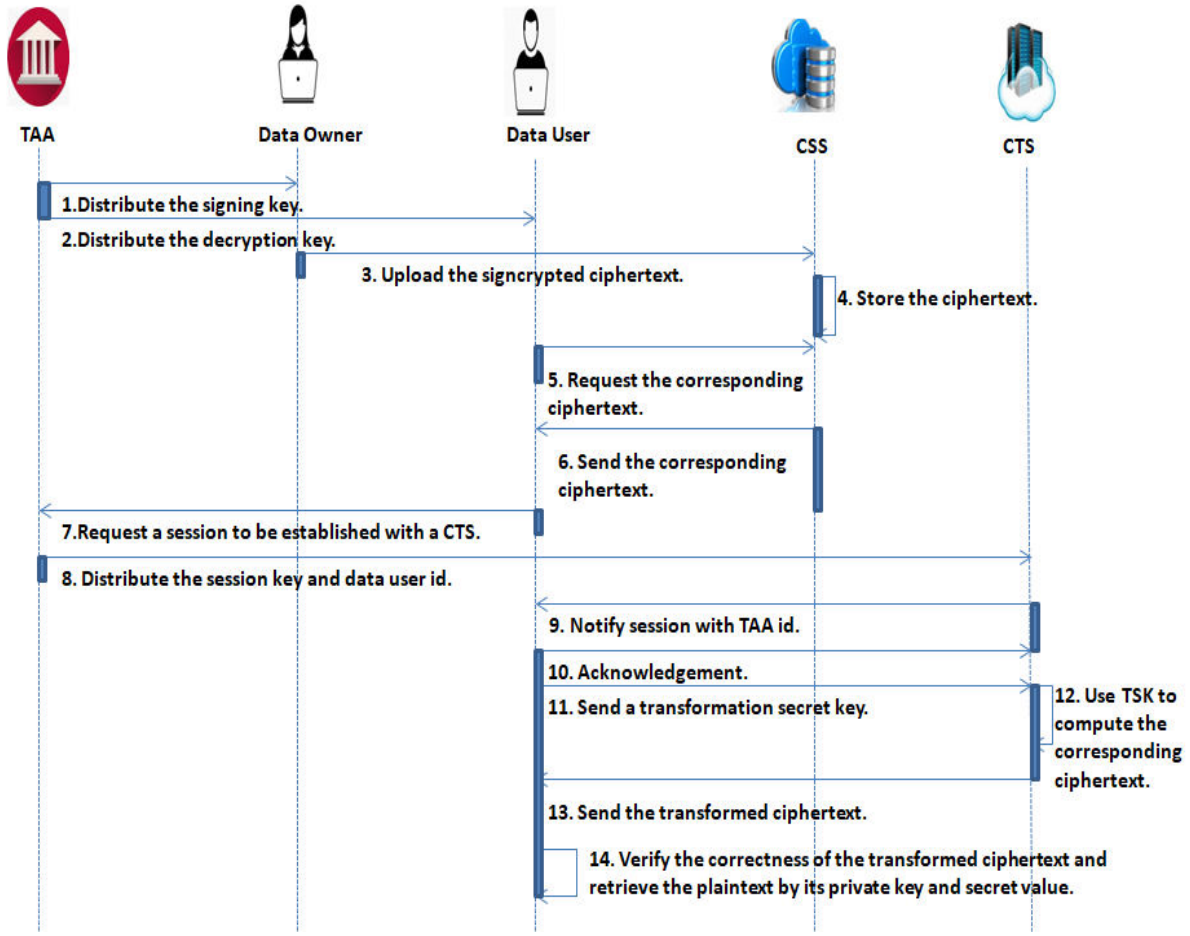

Figure 2: High Level Description of CP-ABSc-ODs

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

IV. RESULT AND DISCUSSION

The proposed scheme CP-ABSc-ODs is implemented in Java platform and the results are compared with an existing CP-ABSC and Triple DES based encryption schemes.

Table 1 shows the signcryption time evaluation of the three schemes based on the number of attributes used and the corresponding graph is shown in Figure 3.

Table 1: Evaluation of signcryption time

No. of Attributes	Proposed Signcryption time	Signcryption Time foe Existing User Key Encryption	Signcryption Time for Existing TDES Encryption
2	487	573	672
4	625	712	785
6	796	889	989
8	869	927	987
10	1085	1171	1243
12	1254	1318	1378
14	1396	1455	1555
16	1498	1573	1638
18	1617	1712	1774
20	1809	1880	1956

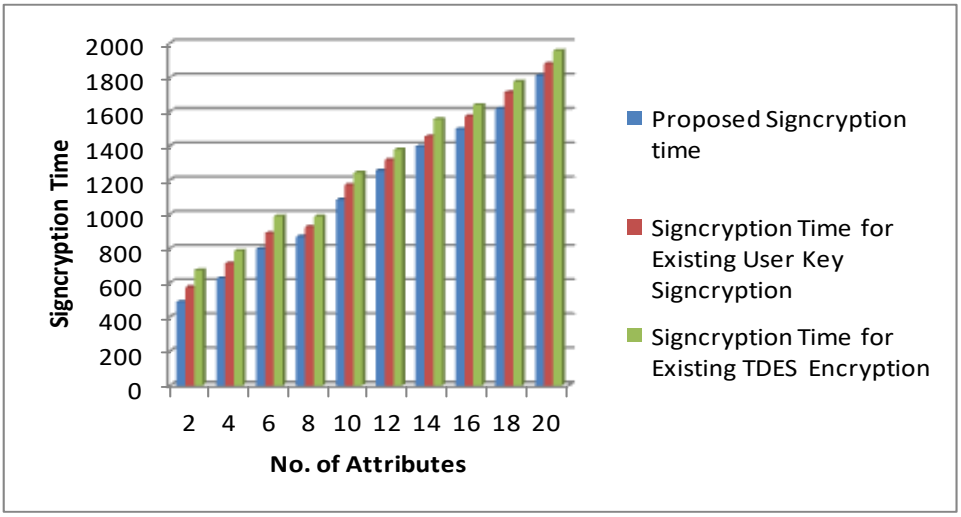

Figure 3: Graphical representation od signcryption time evaluation

Table 2 shows the different designcryption time for a given number of attributes used. It is observed that the number of attributes involved is proportional to the designcryption time involved. Figure 4 shows its corresponding graphical representation. It can be observed that the designcryption time is lesser to that of the existing schemes.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Table 2: Designcryption time evaluation

No. of Attributes	Proposed Designcryption Time	Designcryption Time for Existing User Key Signcryption	Designcryption Time for Existing Time for Existing TDES Encryption
2	1125	1188	1256
4	1845	1940	1993
6	2156	2206	2256
8	2658	2719	2787
10	3105	3170	3264
12	3645	3722	3775
14	3948	4034	4114
16	4068	4155	4214
18	4185	4255	4349
20	4369	4451	4547

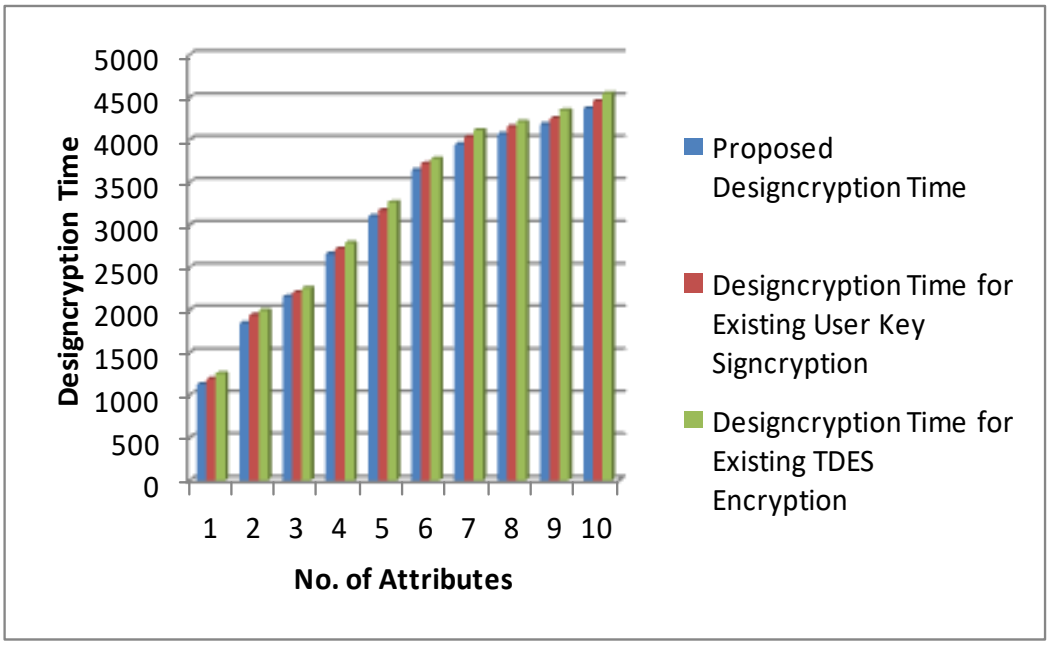

Figure 4: Graphical representation of designcryption time evaluation

Table 3 shows the key response time for the three schemes by varying the number of attributes. Figure 5 shows the respective graphical representation of key response time evaluation.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Table 3: Key response time evaluation

No. of Attributes	Proposed Key Response Time	Key Response Time for Existing User Key Signcryption	Key Response Time for Existing TDES Encryption
2	12	21	22
4	13	21	23
6	14	22	24
8	12	19	22
10	14	19	25
12	13	19	21
14	14	21	22
16	12	21	21
18	15	20	22
20	12	19	21

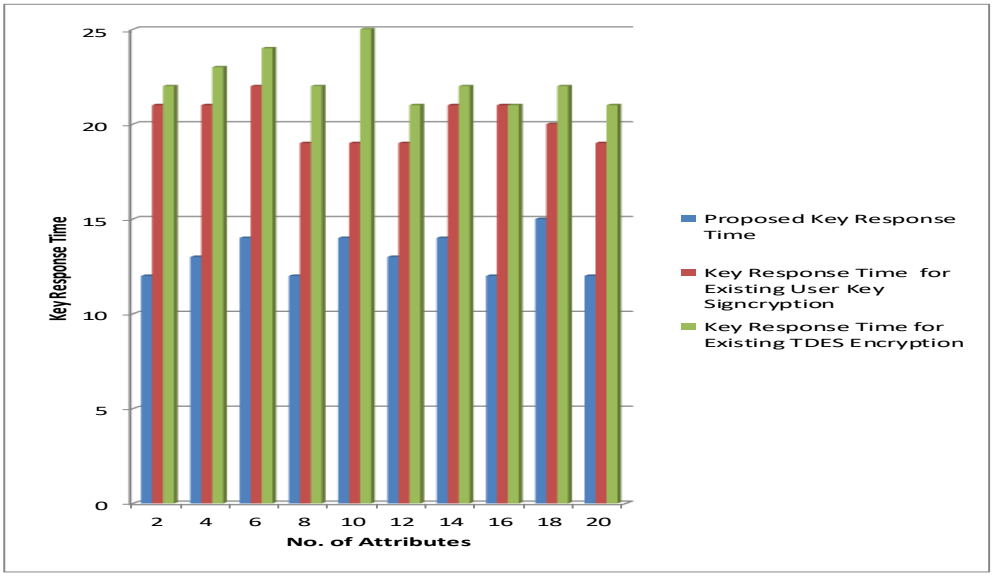

Figure 5: Key response time evaluation.

V. CONCLUSION

The usage of cloud and its services are becoming almost inseparable in almost all our day-to-day activities. The cloud characteristics like resource sharing, on-demand self-service, metered service, fast and desired elasticity attracts every single internet user to become the cloud users and yet the characteristics like geographic distribution and multitenancy arises security issues like data confidentiality and privacy. In this paper, we have presented an overview of the various encryption techniques that are quite promising in providing data confidentiality. The various techniques are compared that gives us a clear view on how to choose the needed encryption scheme to suit our requirement in the cloud. From the observation it is understood that the existing encryption techniques are having heavy computational overhead and so the computation cost is high and also most techniques do not provide efficient operations to be done on encrypted data.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

On demand self services of cloud has offered a wide spectrum of opportunities to every cloud user. Opportunities always bring some kind of threat along with them but the users have to make a trade off and decide on what is the need of the hour and how the tackle the threat intelligently and wisely. The cloud researchers are providing a large number of options to make use of cloud storage without the threat of exposing the critical information with the help of innumerable encryption techniques.

The proposed work entitled CP-ABSc-ODs in this paper is one such efficient signcryption scheme that ensures accountability, verifiability and confidentiality to critical private data. Outsourcing the designcryption phase to CTS reduces computational overhead of the user considerably. Analysis of time usage involved in CP-ABSc-ODs scheme is done. If there is a suspicious activity, the related stakeholders will be instantly notified so that they can act to the situation as needed. In future, this work can be enhanced to include revocation of users when there is a change in the access policy or an ex-user is trying to gain access to confidential data. By doing so data sharing in cloud can be a pleasant experience without the fear of data being exposed to others.

REFERENCES

[1] National Institute of Standards and Technology. The NIST definition of cloud computing; 2011. <http://www.nist.gov/itl/cloud/upload/cloud-defv15.
pdf> [retrieved 24.09.18].
[2] Rong Chunming, Nguyen Son T. Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011); 2011.
[3] Rong C et al. Beyond lightning: A survey on security challenges in cloud computing. Computers and Electrical Engineering(2012). http://dx.doi.org/10.1016/j.compeleceng.2012.04.015.
[4] Wang Z, Sun G, Chen D. A new definition of homomorphic signature for identity management in mobile cloud computing, Journal of Computer and System Sciences, Vol. 80, N0. 3, 2014, pp. 546-553.
[5]Yakoubov S, Gadepally V, Schear N, Shen E, Yerukhimovich A. A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud, IEEE High Performance Extreme Computing Conference (HPEC), 2014, pp. 1–6.
[6] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. 29th Conference on Information Communications, San Diego, CA, USA, 2010, pp. 534-542.
[7] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2007, pp. 321-334.
[8] N. Attrapadung, B. Libert, and E. De Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Public Key Cryptography–PKC 2011. Springer, 2011, pp. 90–108.
[9] Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing, Information Sciences, Vol. 258, 2014, pp. 371-386.
[10]Debasis Das, "Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation", Das, D. (2018). Secure cloud computing algorithm using homomorphic encryption and multi-party computation. 2018 International Conference on Information Networking (ICOIN). doi:10.1109/icoin.2018.8343147
[11]D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in Proc. of IEEE S&P'00, 2000.
[12] R. A. Popa, F. H. Li, and N. Zeldovich, "An Ideal-Security Protocol for Order-Preserving Encoding," in Proc. of IEEE S&P'13, 2013.
[13]N. Chenette, K. Lewi, S. A. Weis, and D. J. Wu, "Practical order-revealing encryption with limited leakage," in Proc. of FSE'16, 2016.
[14] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neil, "Order-Preserving Symmetric Encryption," in Proc. of EUROCRYPT'09, 2009.
[15] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and Attribute Factors Combined Access Control on Time-Sensitive Data in Public Cloud," Proc. 2015 IEEE Global Communications Conference (GLOBECOM 2015), pp. 1-6, 2015.
[16] Huang, Q., Yang, Y., & Fu, J. (2018). Secure Data Group Sharing and Dissemination with Attribute and Time Conditions in Public Cloud. IEEE Transactions on Services Computing, 1–1. doi:10.1109/tsc.2018.2850344
[17] Deng, F., Wang, Y., Peng, L., Xiong, H., Geng, J., & Qin, Z. (2018). "Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records", IEEE Access, 6, 39473–39486. oi:10.1109/access.2018.2843778.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

[18] Quan, H., Wang, B., Zhang, Y., & Wu, G. (2018). Efficient and Secure Top-k Queries With Top Order-Preserving Encryption. IEEE Access, 6, 31525–31540. doi:10.1109/access.2018.2847307.

[19] Huang, Q., Yue, W., He, Y., & Yang, Y. (2018). Secure Identity-Based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing. IEEE Access, 6, 36584–36594. doi:10.1109/access.2018.2852784.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details