Research Article

CP-ABSc-AODs : CIPHERTEXT-POLICY ATTRIBUTE-BASED SIGNCRYPTION WITH ACCOUNTABLE OUTSOURCED DESIGNCRYPTION - AN ENHANCED SECURE DATA SHARING SCHEME

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

Abstract

Cloud computing is becoming the powerful and popular model to all internet users as they can use the required resources from the available pool. As users are freed from operational and maintenance costs, it is very cheaper to pay only for what they use. Also IT companies started migrating their huge data and applications to the cloud which in turn is managed by the cloud service provider (CSP). The CSP may not be trustable and so data owners as well as users require the stored data to be secured even from illegal access from the CSP itself. Since cloud geographically disperses the content while storing, data location is hidden and data can be vulnerable questioning the confidentiality and integrity of the data. Achieving confidentiality requires to follow cryptographic approaches to give access only to authorized and intended users. This paper proposes an efficient Ciphertext-Policy Attribute-Based Signcryption with Accountable Outsourced Designcryption (CP-ABSc-AODs) to securely share data that supports confidentiality, accurate access control, authenticity, message integrity as well as sender privacy. Signer's anonymity is maintained using signcryption. Designcryption is a complicated process with heavy computational overhead and so it is outsourced to a Ciphertext Transformation Server benefiting the user with minimal computational overhead. This paper also concludes that the additional communication overhead due to outsourcing is tolerable.

Keywords— Accountability, Confidentiality, Outsourced designcryption, Privacy, Signcryption.

1. INTRODUCTION

All over the world, the usage of internet based computing has increased and the COVID'19 pandemic situation has proved the importance of cloud based computations and storage. People have started to work from home and schooling have shifted their attention to virtual classrooms. With lockdown the usage of internet has increased drastically and huge amount of personal and official data are roaming around the globe and is stored in some random geographical locations by the cloud service provider [1]. The advancement in 4G technology and high speed internet connection has attracted more users to the cloud.

[1]Research Scholar in Computer Science, Noorul Islam Centre for Higher Education,Kumaracoil-629180, India
[2]Director /Academic Affairs,Department of CSE, Noorul Islam Centre for Higher Education,Kumaracoil-629180, India
* Corresponding author e-mail: reenavargheese11@gmail.com

Now everyone started using cloud on a daily basis for computation, storage, purchase and entertaintment. This situation demands the need to maintain data confidentiality. Reena et al. [2] have compared various encryption schemes including Identity-Based Encryption, Attribute-Based Encryption, Hierarchical Attribute-Based Encryption, Identity-Based Broadcast Encryption, Searchable Encryption, Homomorphic Encryption, Fully Homomorphic Encryption that help to achieve confidentiality.

2. RELATED WORK

Huge data archives are available in the cloud and require information in advance to secure data confidentiality before sharing with third party websites or downloading to the user’s site. The Internet will also need data on those sites [3]. The drawback of traditional encryption is that data can be shared only at a high level (for example, by giving the other party a private key) [4]. Therefore, encryption based on attributes is preferred to encrypt data using appropriate access rights and conditions associated with keys and passwords. Attribute-based encryption (ABE) is flexible to users to exchange and manage sensitive data than the traditional encryption schemes [5]. Also, whenever users are requesting for sensitive data, there should be proper mechanisms and policies that enable them to access information satisfying a privacy policy [6].

ABE techniques provide such features hence are very attractive in cloud storage. However, the demerits of standard ABE techniques are their relatively high cryptographic size and high cost of destruction, and this problem is especially acute for limited resource devices such as mobile devices. Under the ABE scheme, code size and decoding costs increase as access structures / policies become more complex [7].

Yu et al. [8] have implemented ABE scheme that make use of the user’s attribute set and an access policy. ABE is categorized into two types: Ciphertext-policy attribute-based encryption (CP-ABE) and Key-policy attribute-based encryption (KP-ABE) depending on the ciphertext and private key [9]. An Attribute-Based Signcryption scheme is introduced that combines attribute-based signatures (ABS) and encryption. ABS ensures the signer’s anonymity because the identity of the signer is not revealed. Deng et al. suggested a CP-OABSC scheme that outsources decryption process and enables verification of signer thus enabling authenticity to be available [7].

Recent scheme named CP-ABSC (Ciphertext-Policy Attribute-Based Signcryption) has been proposed to secure personal health records of patients on cloud, wherein confidentiality against supposedly coded attacks selected in the predicting model must be required [10]. In 2007, Betencourt et al. developed the first CP-ABE scheme. In 2008, Waters proposed the most important CP-ABE as an entry strategy using LSSS (linear secret-sharing schemes) and demonstrated the security of a discretionary model. In current ABE frameworks, information access strategies are generally communicated in LSSS, which is rich in keys and passwords [11]. In 2010, Lewko suggested the first fully secure ABE circuits. Lewko et al. used a dual system encryption technique to implement functional encryption to bring a wider possibility to share encrypted data [12].

CP-ABE is found to be more suitable for outsourcing data architecture than Key Policy-ABE as owner attributes are utilized in the former. User revocation facility to be used when required was introduced [13]. Mayur N. Ghuge et al. introduced a CP-ABE scheme to have minimal computation overhead during encryption by using short ciphertext that will reduce the decryption time as the number of pairing operations will be considerably minimized [14]. Tamizharasi et al.

suggested a scalable CP-ABE method for grouping users in an order based on their common attributes. This is stored as a user attribute relationship table that helps to manage the overall processing well [15]. Praveen Kumar et al. came up with a scheme entitled Hidden Policy CP-ABE with conjunctive keyword search (HP-CPABCK). The data owner can choose a particular server for testing in order to defend from the offline keyword guessing attacks [16].

On the other hand, a notable demerit of ABE is the computational cost for decryption which proportionally increases along with the complexity of the access structure. Therefore, it becomes essential to enhance the efficiency of computational work before deployment. As a result, the outsourcing concept on decryption and without disclosing the private key was introduced [17]. Another scheme, Fully Outsourced ABE (FOABE), provides a safer key generation, encryption and decryption through outsourcing, but tends to increase communication cost on both client as well as PKG [18]. In our proposed work, we introduce an efficient Ciphertext-Policy Attribute-Based Signcryption with Accountable Outsourced Designcryption (CP-ABSc-AODs) scheme that provides verifiability and accountability for secure data sharing to reduce the overall computation cost.

Section 3 briefs the problem definition. Section 4 highlights the methodology of the proposed work. Section 5 provides the result and discussion. Section 6 gives the conclusion and direction to proceed research in future.

3. PROBLEM DEFINITION

The two technical challenges identified while using cloud storage are:

- The cost for generating keys and performing encryption and decryption is directly proportional to the complexity of the access policy, so the major concern is how to perform ABE that includes outsourcing for key generation, encryption and decryption simultaneously. It must also prevent the public users from finding out the secret keys or confidential data.
- Outsourcing reduces the computation cost for the user and PKG, but it introduces additional communication costs. Therefore the other concern is to decide on how the cost of communication between the user and the PKG can be optimized.

So keeping these challenges in mind, an efficient Ciphertext-Policy Attribute-Based Signcryption with Accountable Outsourced Designcryption (CP-ABSc-AODs) scheme for the cloud-based framework is proposed.

4. PROPOSED METHODOLOGY

In this paper, a scheme that performs outsourcing of designcryption namely Ciphertext-Policy Attribute-Based Signcryption with Accountable Outsourced Designcryption (CP-ABSc-AODs) is introduced to solve the problems of increased computation costs for user and the PKG. First, we formalize a structure of the CP-ABSc-AODs. The feature enabling to verify the outsourced decryption and server-aided signature in a controlled environment makes this method a unique and advantageous one.

4.1. Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE) is a promising cryptographic scheme that provides an accurate access control while accessing confidential or sensitive data but there is a heavy computational complexity of key issuance and encryption. Some solutions prefer to outsource complex computations to a third-party cloud but they fail to address the verifiability of the obtained results. Outsourcing enables users to perform high storage or computation intensive tasks even if their resources are very limited.

4.2. Attribute-Based Signature (ABS)

ABS is an extension of identity-based signature scheme proposed and formalized by Shamir where signer's identity is described using a set of relevant attributes. Fuzzy identity-based signature scheme enables data owners to generate signatures with a subset of the attributes they own. The first ABS scheme achieves user's privacy by making the user to sign a document using his/her subset of attributes. Initially the ABS scheme supporting a powerful set of predicates involving AND, OR and threshold gates was formally introduced. But the security of this scheme is feeble. Construction of threshold attribute-based signature is applied to both small and large attribute universe. In this method, a document is signed using attributes subset while the verification of signature is validated if the set of attributes used in signing is nearly close to the set of attributes that are used to verify.

4.3. Encryption with Ciphertext Policy ABE (CP-ABE)

An attribute authority issues private key depending on user's attributes. Using logic gates on the attributes, a tree called the access policy is formed. In order to decrypt, the attributes of the user must satisfy this policy. Even though security is improved, a central authority is needed for key issuance. Also performing any operations on the encrypted data by the users is not possible.

4.4. Signcryption with Ciphertext Policy ABE (CP-ABSC)

In CP-ABSC, initially the data is signed and then encryption is done using CP-ABE by the data owner. This scheme achieves confidentiality, signer's privacy, accurate access control, authenticity and verifiability simultaneously. Still, the cost of computation is considerably high for data users.

4.5. Ciphertext-Policy Attribute-Based Signcryption with Accountable Outsourced Designcryption (CP-ABSc-AODs)

The CP-ABSc-AODs outsources the decryption process. Also verification of the signature is done. Hence the computation cost for the user is considerably reduced. On the other side, since both decryption and signature verification are done at the cloud server end, the computational overhead is high on the server side.

The CP-ABSc-AODs scheme includes four major phases:

System Initialization

1. Select a prime p, the generators g, and g_2 for G_1 and G_2, respectively and a bilinear mapping $e: G_1 \times G_2 \rightarrow G_3$.
2. Choose two random exponents $\alpha, \beta \in Z_p$.
3. Select a hash function $H_1 : \{0,1\}^* \rightarrow Z_p$ this function H is viewed as a random oracle.
4. Publish the public parameters given by $P_k = (p, G_1, G_2, H_1, g_1, g_2, h = g_1^{\beta}, t = e(g_1, g_2)^{\alpha})$
5. Calculate MSK=($P_k = (\beta, g_2^{\alpha})$)

Key Generation (MSK, S)

Input: The master secret key MSK and an attribute set S belonging to an entity.

1. Select random numbers $r_{en}, r_{sn \in Z_p}$

2. Compute the secret key component $Den = g_2 \frac{(\alpha + r_{en})}{\beta}$ and signing key $K_{sign} = g_2 \frac{(\alpha + r_{en})}{\beta}$
3. For each attribute $j \in s$ do
4. Select a random number $r_j \in Z_P$
5. Compute the secret key component $D_j = g_2^{ren} . g_2^{(H_1(j).r_j)} and D'j = g_2^{rj}$
6. End for
7. The secret key Sk for designcryption $Sk = (Den, \forall_j \in s : D_j, D'j)$
8. Compute the verification $key : Kver = g_2^{rsn}$
9. Send Sk and K_{sign} to the owner of the attribute set s, and publish K_{ver} for others to verify the owner of S.

Signcryption (M, T, K_{sign})

Inputs: The public parameter PK; plaintext message M; the tree T rooted at node R specifying the access control policy of message M; and the signing key K_{sign}.

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

Designcryption (CT_{sign}, SK, S)

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

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

2: if $A \neq \perp$ then

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

4: end if

5: Compute

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

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

7: return $M = M'$

8: end if

9: Return ⊥

The architecture diagram of the proposed work is shown in Figure 1. Data owners signcrypt their personal data and upload it to a fully trusted Cloud Storage Server (CSS). When a user needs access to the data stored on the CSS, his/her own attribute set must be used to check if the access policy is satisfied or not. Also, the user establishes a session with a semi-trusted cloud server used for ciphertext transformation named the Ciphertext Transformation Server (CTS) and requests for transformation. At last, the CTS gives back a transformed ciphertext. Meanwhile, the correctness of transformation ciphertext can be verified by the user and retrieve plaintext by using its private key and transformation related secret value. If any discrepancies are found during designcryption, then the data user can report immediately to the TAA for further legal action.

The high level description of the Ciphertext-Policy Attribute-Based Signcryption With Accountable Outsourced Designcryption (CP-ABSc-AODs) is shown in Figure 2.

A session is used between the data user and the CTS.

- A session can be used to encrypt and decrypt messages that are stored secretively in a device.
- If the ciphertext is tampered then decryption fails while checking for authentication.
- A session must match for a particular encryptiona and decryption of a message.
- Always a unique session ID is generated to identify a session.
- Keys used during a session might be destroyed in order to have forward secrecy.

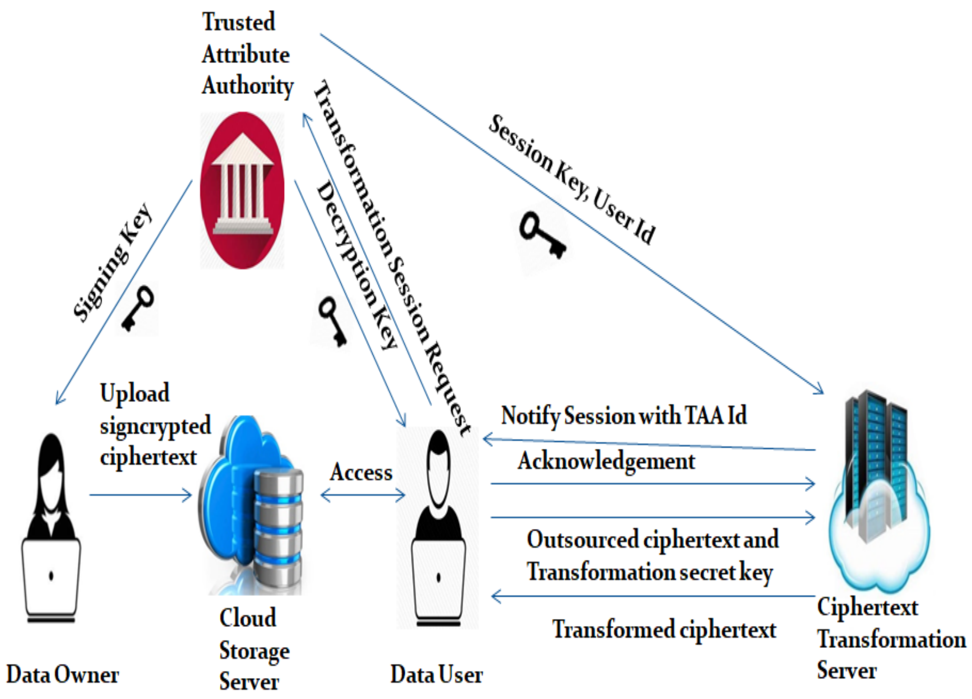

Figure 1: Architecture Diagram of Ciphertext-Policy Attribute-Based Signcryption with Accountable Outsourced Designcryption (CP-ABSc-AODs)

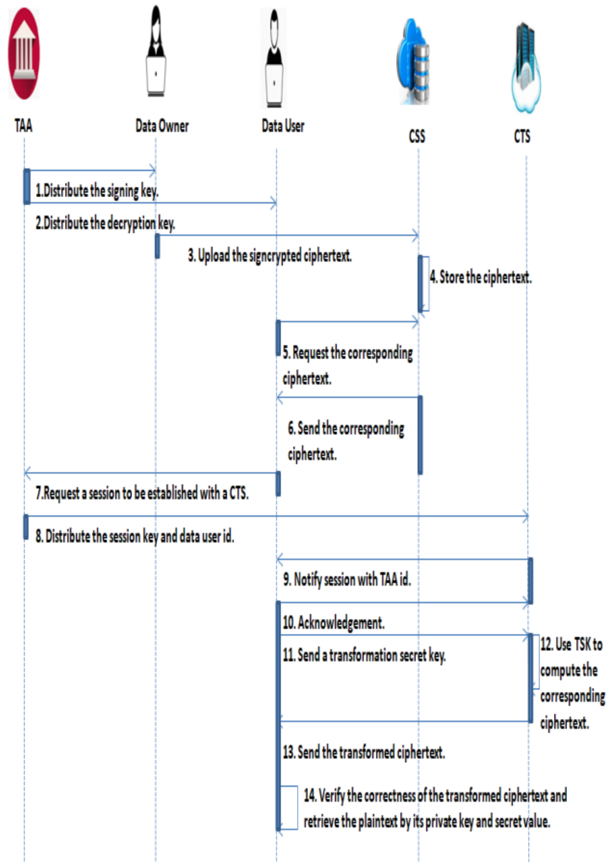
TAA
Data Owner
Data User
CSS
CTS
1.Distribute the signing key.
2.Distribute the decryption key.
3. Upload the signcrypted ciphertext.
4. Store the ciphertext.
5. Request the corresponding ciphertext.
6. Send the corresponding ciphertext.
7.Request a session to be established with a CTS.
8. Distribute the session key and data user id.
9. Notify session with TAA id.
10. Acknowledgement.
11. Send a transformation secret key.
12. Use TSK to compute the corresponding ciphertext.
13. Send the transformed ciphertext.
14. Verify the correctness of the transformed ciphertext and retrieve the plaintext by its private key and secret value.

Figure 2: High Level Description of Ciphertext-Policy Attribute-Based Signcryption with Accountable Outsourced Designcryption (CP-ABSc-AODs)

5. RESULT AND DISCUSSION

An innovative secured sharing of personal data using CP-ABSc-AODs is achieved in the Java work platform. The values of encryption and signcryption are also estimated and its average values are contrasted with those of the current methods.

The research work compares the working of the new CP-ABSc-AODs protocol, an existing CP-ABSC and TDES (Triple DES) based signcryption schemes.

The table below illustrates the comparison of the proposed and existing research works. Table 1 reveals the signcryption time taken by the three schemes with respect to the varying number of attributes considered to signcrypt the data. Its corresponding graph is shown in Figure 3. Table 1 is tabulated in the following section.

Table 1: Signcryption time evaluation in comparison of proposed and existing schemes

No. of Attributes	**Proposed Signcryption time**	**Signcryption Time for Existing User Key Signcryption**	**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

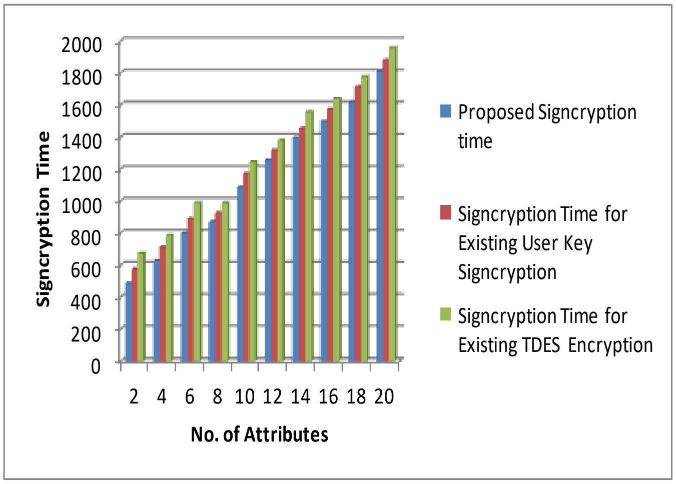

Figure 3: Graphical representation of signcryption time evaluation in comparison of proposed and existing schemes

In table 2, the proposed scheme, the existing user key signcryption scheme and Triple DES scheme used are showing different designcryption time for the same number of attributes utilized. It is found that there is a direct relationship between the designcryption process and the number of attributes involved.

Table 2: Designcryption time evaluation in comparison of proposed and existing schemes

No of Attributes	Proposed Designcryption Time	Designcryption Time for Existing User Key Signcryption	Designcryption 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 shows its relevant graph. Again, the cost of designcryption for the proposed scheme is found out to be lesser than that of other existing schemes.

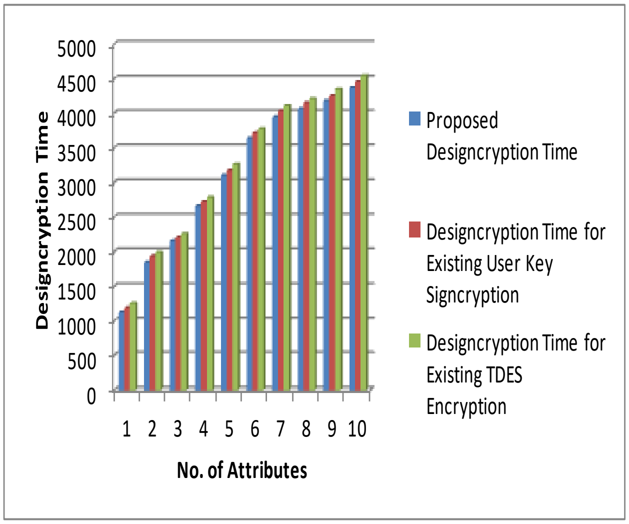

Figure 4: Graphical representation of designcryption time evaluation in comparison of proposed and existing schemes

Table 3 shows the key response time for the above mentioned schemes with varying number of attributes and the corresponding graph is shown in Figure 5.

Table 3: Comparison of proposed and existing key response time

No of Attributes	Proposed Key Response Time	Key Response Time for Existing	Key Response Time for Existing

		User Key Signcryption	**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

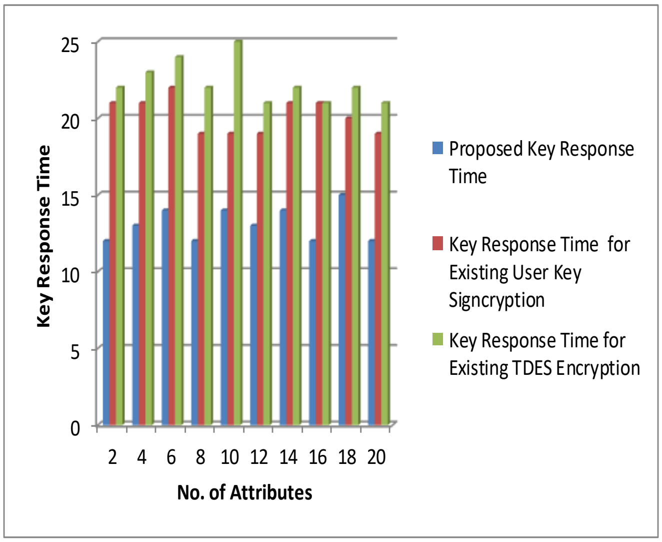

Figure 5: Graphical representation of key response time evaluation in comparison of proposed and existing schemes.

6. CONCLUSION AND FUTURE WORK

Every day the usage of cloud is exploding and in this online era a lot of private data are shared simultaneously that may be accidentally or purposefully tampered with. Hence confidentiality, integrity and accountability are of prime concern to every cloud user. Collusion attacks may also be there. So there is a need for a protocol that provides utmost security to the user. Also it must reduce the computation overhead that will occur normally at the user’s side.

In this work, an innovative signcryption technique named CP-ABSc-AODs is proposed, which provides confidentiality, verification and accountability for sharing private data where designcryption process is outsourced to a semi-trusted cloud transformation server. The time usage for signcryption, designcryption and key response of CP-ABSc-AODs is analyzed. The proposed protocol uses CP-ABE cryptographic primitive to ensure data confidentiality; it is based on a signature verification to guarantee the integrity of the messages received. In addition, in case of malicious activity, the corresponding stakeholders will know it immediately and so can take measures accordingly. As a future work, this work can be improvised to include the user revocation when the access policies change or some ex-users illegally attempt to gain access are to be taken care of legally and henceforth the proposed system can work better in the cloud data sharing system in terms of security and efficiency.

REFERENCES

[1] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, “Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption” , IEEE Trans. Depend. Sec. Comput., vol. 13, no. 5, pp. 533–546, May 2016.

[2] V. Reena Catherine, A. Shajin Nargunam, “Encryption Techniques to Ensure Data Confidentiality in Cloud”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-11S, pp.1047 to 1049, Sep 2019.

[3] S. Lin, R. Zhang, H. Ma, and M. Wang, ‘‘Revisiting attribute-based encryption with verifiable outsourced decryption,’’ IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2119–2130, Oct. 2015.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ‘‘Attribute-based encryption for fine-grained access control of encrypted data,’’ In Proceedings of 13th ACM Conference on Cloud Computing Communication Security, pp. 89-98, 2006.

[5] A. Lewko, B. Waters, ‘‘Unbounded HIBE and attribute-based encryption’’, In Proceedings of Advances in Cryptology EUROCRYPT, Vol. 6632, Berlin, Germany: Springer, 2011, pp. 547–567.

[6] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute based encryption’’, In Proceeding of IEEE Symposium Security Privacy (SP), pp. 321–334, May 2007.

[7] F. Deng, Y. Wang, L. Peng, H. Xiong, J. Geng and Z. Qin, "Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records," In Proceedings of IEEE Access, vol. 6, pp. 39473-39486, 2018.

[8] 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.

[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, ‘‘Attribute-based encryption with verifiable outsourced decryption’’, In Proceedings of IEEE Transaction on Inf. Forensics Security, Vol. 8, No. 8, pp. 1343–1354, Aug. 2013.

[10] Y. S. Rao, ‘‘A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing’’, In Proceedings of Future General Computer System, vol. 67, pp. 133–151, Feb 2017.

[11] H. Wang, D. He, J. Shen, Z. Zheng, C. Zhao, and M. Zhao, ‘‘Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing’’, Soft Computing, Vol. 21, No. 24, pp. 7325–7335 , 2016.

[12] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ‘‘Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,’’ in Advances in Cryptology—EUROCRYPT, vol. 6110. Berlin, Germany: Springer, 2010, pp. 62–91.

[13] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, ‘‘Flexible and fine-grained attribute-based data storage in cloud computing’’, In Proceedings of IEEE Transaction. Services Computing, Vol. 10, no. 5, pp. 785–796, Sep/Oct. 2016.

[14] Mayur N. Ghuge, Dr. Prashant N. Chatur, "Collaborative Key Management in Ciphertext Policy Attribute Based Encryption for Cloud", In Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies, pp. 156-158, 2018.

[15] G.S.Tamizharasi, Balamurugan, "Scalable and Efficient Attribute based Encryption Scheme for Point to Multi-Point Communication in Cloud Computing", In Proceedings of IEEE International Conference on Inventive Computation Technologies (ICICT), pp. 1 to 4, Aug 2016.

[16] P.Praveen Kumar, P.Syam Kumar, P.J.A.Alphonse, "Encryption for Big Data Access Control in Cloud Computing", In Proceedings of Ninth International Conference on Advanced Computing, pp. 114-120, 2017.

[17]J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, ‘‘Securely outsourcing attribute-based encryption with checkability,’’ In Proceedings of IEEE Transaction Parallel Distributed System, Vol. 25, No. 8, pp. 2201–2210, Aug. 2014.

[18] R. Zhang, H. Ma, and Y. Lu, ‘‘Fine-grained access control system based on fully outsourced attribute-based encryption’’, In Proceedings of J. System Software, vol. 125, pp. 344–353, Mar. 2017.