Paper2

By TABASSUM MAKTUM

WORD COUNT	4805	TIME SUBMITTED	03-JUL-2021 09:28PM
		PAPER ID	74083246

The Trusted Hierarchical Access Structure based Encryption Scheme for Cloud Computing

Abstract

Cloud computing delivers various technology resources and services to users over internet. At present many businesses and individual users are adopting cloud services to take benefit of less time, less cost, less management and maintenance. Still, security is the primary issue that must be tackled and efficient solutions to be developed to securely store data with cloud environment. One of the security issues is access control mechanism that guarantees data is access by authorized users only. The most widely used access control method includes Ciphertext Policy based Attribute based Encryption (CP-ABE), which is encrypted access control scheme. In order to ensure trustworthy and encrypted access control, a Trusted Hierarchical Access Structure based Encryption scheme is proposed in this paper. The proposed scheme uses hierarchical access structure to encrypt multiple messages and avoid generation of many ciphertexts. It allows decryption of message even though complete access structure is not satisfied by the associated set of attributes. On the basis of, which part of access structure is satisfied, the corresponding message is decrypted. Thus, it will be computationally efficient and also saves space required to store multiple ciphertexts. The trust evaluation component is also integrated with the proposed access control mechanism. An efficient method to assign trust level for service providers and data uses is also proposed in the paper. The paper also presents performance analysis of proposed scheme by comparing with traditional scheme.

***Keywords**: Attributes, Trust, Cloud Computing, Access Control.*

1. Introduction

In recent days, many organizations are adopting and integrating cloud computing with their traditional infrastructure. Due to this change, there arises a need to develop appropriate solutions to deal with security threats to cloud computing. The security concern arises as the data is stored and handled by the third party service provider. The data owners will have limited control and visibility over the data. As cloud computing is recently emerged paradigm there exists many issues and uncertainty for applying security solutions at various level such as host level, network level, data level and application level. The traditional security solutions are not sufficient for cloud computing because of its large scale, distributed and heterogeneous environment. The topmost threats to cloud security include unauthorized access, mis-configurations, hijacking, malware, phishing attacks etc.

The major challenge associated with cloud computing, which need to addressed, is to ensure secure and authorized access control. As entire data is stored with the third party cloud service provider and available over the public network, it is important to ensure that the data is accessed by authorized users only. The traditional authentication and access control solutions are not fully sufficient for cloud environment. Hence, providing fine-grained and secure access control mechanism for cloud is an important research issue. In this paper, a trusted encrypted access control scheme is proposed for cloud computing. The encrypted access control is based on the Identity based Encryption (IBE) (Shamir, 1985) where the message is encrypted using the identity of the user. The Attribute based Encryption (ABE) (Sahai and Waters, 2005) is presented as application of the traditional IBE scheme. In ABE, attributes of the user and an access policy is used to ensure fine-grained access control. The access policy is built with combinations of different threshold gates and user attributes. The data is made available to the user, only when his/her attributes satisfies the predefined access structure. In literature there are two different forms of ABE schemes available, such as Key-Policy Based Attribute based Encryption (KP-ABE) (Goyal et al., 2006) and Ciphertext Policy Based Attribute based Encryption (CP-ABE) (Bethencourt et al., 2007). These two schemes are different in terms of how attributes and access structure is associated. In case of CP-ABE scheme the attributes are integrated with the key and the access structure is associated with the ciphertext. This will ensure that the key with sufficient attributes can only decrypt the ciphertext that has associated access structure. Whereas in KP-ABE scheme the access structure is integrated with the key and attributes are merged with ciphertext. The KP-AB scheme has one basic limitation that whoever has the ciphertext can decrypt it and there is no way to ensure that only the intended user has decrypted it. In the traditional CP-ABE scheme, separate ciphertext is generated for each message according to the predefined access structure. But, sometimes it is possible that multiple access structures are hierarchically related to each other. Hence it is possible that a hierarchical access structure can be generated, instead of generating multiple separate access structures. This hierarchical access structure can be used to encrypt multiple messages. Also establishing trust among cloud environment and cloud users is of prime importance issue. The service provider should deliver trusted services to the users. Also the users, who are accessing data from cloud, must be trustworthy. Thus it is necessary to integrate trust evaluation along with traditional access control models.

The paper presents the Trusted Hierarchical Access Structure based Encryption (T-HASE) scheme. The major contributions are as follows:

- The hierarchical access structure based scheme to encrypt multiple messages and enable to decrypt the respective message on the basis of how much part of entire access structure is satisfied.

- The trust evaluation scheme that allocates trust levels to service providers on the basis of their performance parameters so that trusted service delivery is ensured.
- The trust evaluation scheme for data users, which evaluates user behaviour, so that only trusted users can access the data shared in cloud environment.

The rest of the paper is organized as follows: The section 2 elaborates existing encrypted access control models for cloud computing. The proposed Trusted Hierarchical Access Structure based Encryption (T-HASE) is explained in section 3. The proposed method is compared with the existing techniques and its performance evaluation is elaborated in section 4. The section 5 represents the conclusion.

2. Related Work

The access control mechanism based on collaboration of users using attributes is proposed in (Alabazar and Kongara, 2020). The information related to the possible collaboration among data users is specified along with the access policies by the owner of the data. The scheme allows multiple users who belong to same group to satisfy the access structure and access the data. The scheme is based on the concept of interpretation hub that is embedded in the access tree. This scheme is based on basic ABE scheme proposed in (Bethencourt et al., 2007) and incorporates interpretation key into the master key generation process. The CP-ABE scheme that deals with multiple different access structure with hierarchical associations is proposed in (He H. et al., 2020). In this paper the CP-ABE system that generates a common access structure from many different access structures that are hierarchically associated is generated. Depending on how much part of the access structure is satisfied, the access of only that part of data is granted to the user. The entire data is available to the user only when entire access structure is satisfied by the attributes of the user. The scheme reduces the computation overhead by combining multiple access structure together and it is bases on linear secret sharing scheme.

The CP-ABE scheme to support dynamic and large set of attributes is presented in (Sravan Kumar, 2020). The scheme also addresses the issue related to identification of malicious user and proposes the traceable scheme, which can find the malicious user or any compromised central authority. The scheme is based on linear secret sharing structure and tree access structure that is expressive and provides fine grained access control. The scheme presented in (Praveen Kumar et al., 2017) is designed for the big data access control in cloud environment. The major contribution of this CP-ABE scheme is it generates shorter ciphertext and needs less number of paring operations. Also, the scheme is computationally efficient as it requires less overhead for encryption and decryption process. The lightweight Attribute based Encryption scheme for Cyber Physical System based on cloud is proposed in (He Q. et al., 2018). The scheme mainly focuses on the scenarios where mobile devices are used for Cyber Physical System. This scheme presents a different ABE technique where no pairing is required for encryption and hence the decryption process also implemented by single pairing operation. Hence the scheme is computationally efficient and is based on proxy services. The Attribute based Encryption technique for hierarchical files, is proposed in (Wang et al., 2016). In this technique the integrated access structure is used to encrypt the multiple shared files, which are hierarchically associated. This approach reduces the ciphertext storage requirement and time required for encryption and decryption. The scheme uses tree access structure and liner secret sharing scheme.

The searchable attribute based authentication scheme is proposed in (Liu and Fan, 2019). This scheme is combination of key policy bases signcyption scheme and attribute based keyword search. It is based on linear secret sharing scheme and provides fine grained access control and authentication. In this scheme the data owner signcrypt the data and generate the encrypted index for the same. The data can be accessed by users by generating trapdoor and they can also validate the received data. The Attribute based Encryption scheme that handles the key escrow problem is proposed in (Sandor er al., 2019). This method is based on decentralized approach with multiple authorities and is applied for mobile cloud computing. In this scheme there is no requirement of centralized authority for key management. In this scheme the cloud user assistant are responsible to communicate with various attribute authorities and to perform the partial decryption task. This will reduce the overhead on data user side and improves performance. The CP-ABE scheme that provides access to data to the multiple data users from different domains is proposed in (Vaanchig et al., 2018). This scheme also addresses the issues related to key escrow problem and efficient revocation scheme. It provides a CP-ABE scheme that solves key escrow problem and provides dual revocation mechanism.

The authors in (De and Ruj, 2020) present a fully decentralized CP-ABE scheme for mobile cloud that outsources the decryption process. In this scheme the heavy computation during encryption process are carried out offline and hence makes encryption process quiet efficient. The proxy server will perform the partial decryption and reduces the overhead due to the decryption process. The data sharing scheme that applies Attribute based Encryption with online/offline strategy is proposed in (Li et al., 2018). This method shifts the costlier computation to offline phase. The online ciphertext is produced by using Chameleon hash function. In order to make decryption process efficient, this method performs the check for illegal ciphertext prior to decryption process. The CP-ABE scheme that incorporates role hierarchies and hierarchical access structure is presented in (Challagidad and Birje, 2020). The users are grouped according their roles/privileges and attributes and the hierarchical structure is created to ensure secure access to the data. This method also supports multiple authority based access control by allowing hierarchical access structure.

Thus, there exist certain methods in literature that apply attribute based encryption for securing access for cloud data. But to ensure trusted and secure access for data stored in cloud, there is need to inculcate mechanism of trust into the encrypted access control. Also traditional attribute based encryption method incurs heavy computation overhead. Hence the paper proposes an integrated method to provide trustworthy and secure access to cloud data that combines trust and encrypted access control with hierarchical access policies. The following sections cover details of the proposed method.

3. Proposed Work

The main goal of this work is to propose an efficient access control technique that supports hierarchical access structure and also to integrate trust based access scheme to ensure secure and trustworthy access to the data stored in cloud storage. The major components of the proposed method are Data owner, Data User, Trust Evaluation Model, Hierarchical Access Structure based Encryption (HASE) and Cloud Service provider. The data owner can store the data in encrypted form in the cloud environment. The data owner can assess the trustworthiness of service provider before transferring data in the cloud environment so that it is guaranteed that the data is managed by trusted resources. The data owner designs hierarchical access structure for multiple files. The hierarchical access structure is created by combining access structures that have some hierarchical relationship among them. This kind of access structure allows encrypting multiple files by using the combined access structure, instead of encrypting them with separate access structures. These hierarchical access structures along with standard Ciphertext Policy Attribute based Encryption (Bethencourt et al., 2007) scheme is used to encrypt the data. While decrypting such ciphertext, if only some part of access structure is satisfied by user's attributes then data related to this much part only is available to user. If complete access structure is satisfied then the complete data is made available to the user. The system model of proposed work is depicted in Fig. 1.

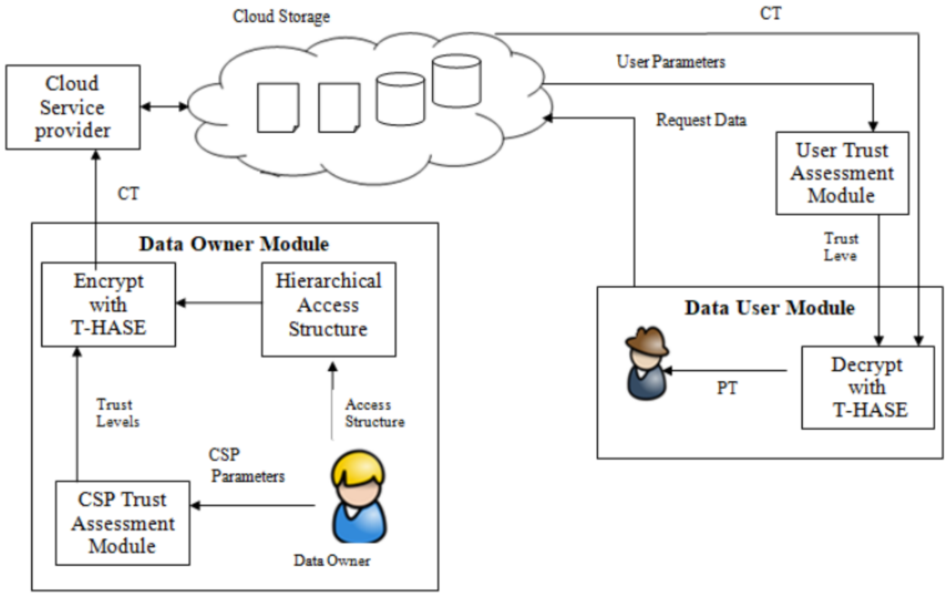

Figure 1: Proposed Scheme Architecture

3.1 Working:

1. Cloud Service Provider will manage all cloud resources and handle all requests from the data owner and data user. It will communicate with data owner module and store the encrypted data into cloud environment. Whenever any user requests the data from the cloud storage, it will communicate with User Trust Assessment module to computer user's trust level. Then transfer the trust level to the Data User module.

2. The Data Owner module is responsible for encrypting the data and transferring the corresponding ciphertext to the cloud environment. It will communicate with the CSP Trust Assessment module to compute the trust level of CSP that is delivering the storage service. If this trust level is above threshold then only the CSP is selected to deliver the service. After selecting an

appropriate and trusted CSP, the module generates hierarchical access control along with the user's trust level embedded in it and uses it to encrypt the data.

3. The Data User module will receive the trust level of user from the trust assessment module and Ciphertext from the CSP. Then it will utilize the user's attribute set to check whether the corresponding access structure is satisfied or not. If yes then the related data is delivered to the user.

3.2 Proposed Trusted Hierarchical Access Structure based Encryption (T-HASE) Scheme

In traditional CP-ABE scheme the attributes are tied with the key and access structure is tied with the ciphertext. While decrypting the ciphertext, it is verified that the user attributes are able to satisfy the mentioned access policy. In general, the attributes of the user satisfies the access structure completely or else it fails to satisfy it. With this approach there will be multiple access structures for multiple files and multiple ciphertext will be generated. If the access structure associated with different files are hierarchically related then it is possible to generate combined access structure for multiple files. Such access structure is considered as hierarchical access structure. It will reduces the number of access structures to be generated and hence the number of ciphertext. Consider there is an Attribute set A :{ 1, 2, 3, 4, 5} and two access structures defined for two different messages are A1 and A2. Here, A1 is {((1 AND (2 OR 3)) AND 4)} AND A2 is {(1 AND (2 OR 3))}. Then a combined hierarchical access structure is for A1 and A2 is considered as, {((1 AND (2 OR 3)) AND 4)}. If any user has attribute set as, {1, 2} then this attribute set will satisfy the partial access structure and the related message will be decrypted for the user. If any other user has attribute set as, {1, 3, 4} then the complete access structure will be satisfied by this attribute set and hence relevant data will be decrypted for this user.

3.2.1 Hierarchical Access Structure based Encryption

The process includes four major steps as setting initial system parameters, generating keys, encryption and decryption. The access structure is built in the form of access tree, where the leaf node has attributes and non-leaf nodes are logical gates like OR, AND etc.

Step 1: This is system initialization step where the Public key and master key is computed. The bilinear group, $\mathbb{G}$ of prime order p with generator g is used. Consider two random elements α and β are selected over $\mathbb{Z}p$.

The public key is computed as PK:

$$PK = \mathbb{G}_0, g, g^{\beta}, e(g,g)^{\alpha}$$

The master key is computed as:

$$MK = g^{\alpha}$$

Step 2: In this step the secret key is computed. Let A is the set of attributes and x is a random element selected over $\mathbb{Z}$. The random element x_j is selected for each attribute a_j.

$$SK = \{(g^{\alpha+x})^{\frac{1}{\beta}}, For\ each\ A_j : D_j = g^{x}.h, \_D_j = g^{x_j}$$

Step 3: The message is encrypted using the public key and the access structure. The random secret s is selected for the root node of the access tree. The polynomial q is associated with each ode in the access tree. Let there are n messages as {m$_1$, m$_2$…m$_n$}. The ciphertext is calculated as :

$$CT = \{m_j.e(g,g)^{\alpha s_j}, h^{s}, For\ each\ leaf\ node\ l : g^{q(0)}, H(attribute(l))^{q(0)}$$

Step 4: The message is decrypted if the user's attribute set satisfies the corresponding access structure. The secret at the particular node must be generated by using the user's attribute set so that the respective message will be decrypted. The ciphertext components and the secret key components are used to decrypt the message.

$$mj = C'_j/(e(h^{s}, (g^{\alpha+x})^{\frac{1}{\beta}})/e(g,g)^{rs_j}$$

3.2.2 Trust Computation Scheme

The proposed method integrates the trust level of user into the access structure used for encrypting the data. This will guarantee trustworthy attribute based access control mechanism for the user's data. The trust levels of CSPs as well as the data users are computed. The assessment of trustworthiness of CSP will ensure that the data is handled by trusted service. In the same way the trustworthiness of data user is computed to ensure that data is utilized by trusted user only. In order to compute trust levels for CSP, different performance parameters are considered, which are maintained as performance monitoring system as performance logs. The performance parameters that are utilized during trust assessment process are response time, success rate, throughput, availability and reliability. The Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method is applied to assign different trust levels to the CSPs and data users. The TOPSIS is one of the most widely used methods for decision making, where multiple criterions are involved. The weights for different performance parameters of CSP are computed by applying Fuzzy-Analytical Hierarchical Process. These weights are used by TOPSIS method while deriving trust levels.

The following steps are followed to assign trust levels to CSP or data users. Consider that there are ***n*** CSPs and ***m*** performance parameters.

Step 1: The performance of CSP is monitored and the values of considered parameters are maintained by the performance monitoring system. The average value of previous ten interactions of corresponding CSP, for each parameter is considered while computing trust level. The evaluation matrix based on these values is computed as:

$$E\_CSP_{nxm} = \begin{matrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ c_{n1} & c_{n2} & \cdots & c_{nm} \end{matrix}$$

Step 2: In this step the normalized evaluation matrix is computed. The normalized value is computed as:

$$E\_CSP_{ij} = E_{CSP_{ij}}/(\sum_{l=1}^{m}(E\_CSP_{lj})^2)^{1/2}$$

Step 3: In this step the weighted normalized evaluation matrix is computed. The weights for all parameters are computed using Fuzzy-AHP method. Here the pair-wise comparison matrix is generated using AHP scale. This matrix indicates the preference f one parameter over the other. Consider that w={w1,w2,…wm} indicates the weight vector for m parameters. The weighted normalized evaluation matrix is computed as:

$$E'\_CSP_i = E\_CSP_{ij} * w_j$$

Step 4: Generate Ideal Solution S*. Here the set of benefit attributes, *A* and set of negative attributes, *A'* is considered to compute ideal solution. The attribute is benefit attribute if its larger value is considered as better and attribute is negative attribute if its smaller value is considered as better. The maximum value of benefit attribute is selected and minimum value of negative attribute is selected as a part of negative ideal solution.

Let there are ***k*** benefit attributes and ***i*** negative attributes such that, ***k+l=m***

$$S^* = \{\max(A_{kj}); \min(A'_{lj})\}$$

Step 5: Generate negative ideal Solution S'. Here also the set of benefit attributes, *A* and set of negative attributes, *A'* is considered. The maximum value of negative attribute is selected and minimum value of benefit attribute is selected as a part of negative ideal solution.

Let there are ***k*** benefit attributes and ***i*** negative attributes such that, ***k+l=m***

$$S' = \{\min(A_{kj}); \max(A'_{lj})\}$$

Step 6: The deviation from ideal solution dS* is computed.

$$dS^*_j = (\sum_{i=1}^{n}(S^*_j - E'\_CSP_{ij})^2)^{1/2}$$

Similarly, the deviation from negative ideal solution dS' is computed.

$$dS'_j = (\sum_{i=1}^{n}(S'_j - E'\_CSP_{ij})^2)^{1/2}$$

Step 7: Finally, the score for each CSP is computed as:

$$S\_CSP_i = dS'_i/(dS'_i + dS^*_i)$$

On the basis of this score the respective trust level is assigned to the CSP. The trust level is assigned as high if the score lies in the range [0.7-1.0] whereas the trust level is assigned as moderate if the score is in range [0.4-0.6]. If the score is in the range [0.0-0.3] then the trust level will be low. The trustworthiness of data user is also computed by considering the behavioural parameters of users. The different parameters to judge user's behaviour include, number of failed logins, attempts to access data that is not permitted, type of data being uploaded , type of data being downloaded etc. The similar process explained in above section is applied to compute trust levels for data users. The user behavioural parameters for different interactions are maintained by the monitoring system and these evidences are utilized to compute trust level using TOPSIS method.

4. Simulation and Results

4.1 Simulation

The proposed T-HASE scheme is implemented based on JPBC library (Caro and Iovino, 2011) and traditional CP-ABE implementation (Bethencourt et al., 2007). The different experiments are conducted to assess the performance of proposed system in terms of accuracy for evaluating trust levels, encryption time and decryption time. The three other methods are also implemented that uses TOPSIS with AHP weights, Fuzzy-AHP based trust evaluation and AHP based trust evaluation. The proposed method is compared with these existing trust evaluation schemes to major its performance. The performance is measured in terms of accuracy in judging the trust levels for both CSP and data users. The proposed hierarchical access structure based method for encrypting messages and providing access control is implemented. The performance of proposed scheme is compared with the traditional CP-ABE scheme in terms of encryption and decryption time.

4.1.1 Simulation Model

The different datasets with varying umber of interactions of CSP and data users are considered while implementing the trust model. The parameters that represent the performance of CSP such as response time, success rate, throughput, availability and reliability are collected. For each parameter, the average value of previous 10 interactions is considered for assigning the trust level to the service provider. The dataset of varying number of interactions such as 100, 500, 1000, 3000 and 5000 is generated and value of each parameter is normalized to range [0-1]. Similarly the parameters that represent user's behaviour are collected and the trust level is computed for each data user. The considered behavioural parameters include number of failed logins, attempts to access data that is not permitted, type of data being uploaded , type of data being downloaded. For these parameters also different datasets with varying number of user interactions are considered. The values of last 10 interactions are considered and these are normalized to [0-1] range. Here also the datasets containing 100, 500, 1000, 3000 and 5000 user interactions are generated. By applying the method explained in section 3 the score is calculated for different interactions of service provider and user. On the basis of these score, the possible trust levels that can be assigned to service provider or user are high, moderate and low.

In order to evaluate performance of the proposed hierarchical access structure based scheme, various access policies are created. The different attributes of users are considered for generating these access policies and the threshold gates that are utilized include AND, OR. The performance is evaluated by varying number of attributes used for generating access tree. The threshold gates that are used to generate access policy include AND and OR gates. The different access policies are created with varying number of attributes and the time required for encryption and decryption of message is measured. Also the number of messages to be considered is varied and time required for encryption and decryption is measured. The proposed method is also evaluated on the basis of amount of storage required for generated ciphertext.

4.2.2 Results and Discussion

The Fig. 2 shows the comparison of proposed scheme with the other methods with respect to accuracy of assigning trust levels to CSP. The accuracy is measured for all methods by varying number of interactions. It can be observed from Fig. 2 that the accuracy for the proposed method is high as compared to other methods for all datasets. Thus, the considered parameters for representing performance of the CSP are appropriate for evaluating trust levels and also the combination of TOPSIS with fuzzy AHP weights is more appropriate.

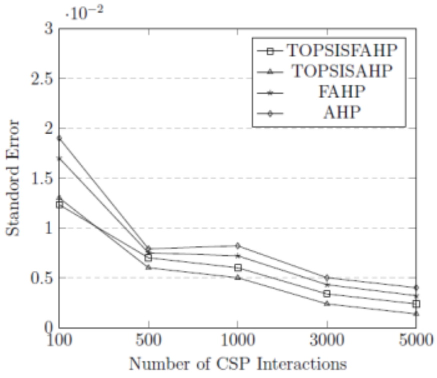

Fig. 2 Comparison of Accuracy of Evaluation of Trust Levels for CSP

The Fig. 3 shows the comparison of proposed scheme with the other methods with respect to accuracy of assigning trust levels to data users. Here also different datasets with varying number of user interactions are considered. The parameters that depict user behaviour are measured and maintained with these interactions. It is observed from the Fig. 3 that the proposed method is more accurate in terms of assigning trust levels to data users. Thus, the selection of behavioural parameters and the computed weights are more appropriate as compared to other methods.

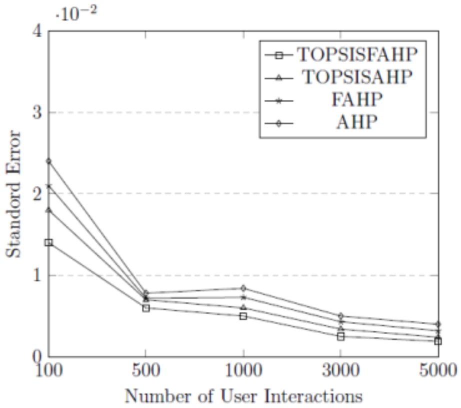

Fig. 3 Comparison of Accuracy of Evaluation of Trust Levels for Users

The Fig. 4 shows the comparison of encryption and decryption time taken by proposed scheme and traditional CP-ABE scheme by varying number of attributes in access policy. It can be observed from the Fig. 4 that the proposed method takes less time as compared to existing scheme.

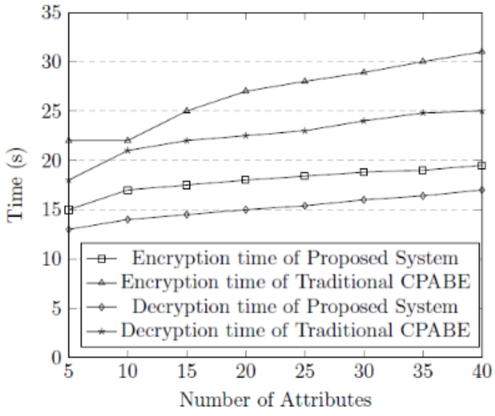

Fig. 4 Comparison of Encryption and Decryption Time

The Fig. 5 represents comparison of encryption and decryption time taken by proposed method and traditional CPABE scheme with respect to number of messages. Here, 10 attributes and access policy with AND and OR gates are considered for evaluating encryption and decryption time. It can be observed from Fig. 5 that the proposed method takes less time for both encryption and decryption as hierarchical access structure is used for multiple different messages.

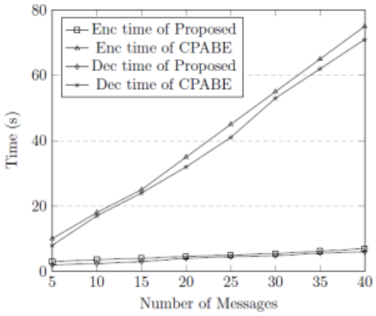

Fig. 5 Comparison of Encryption and Decryption Time

The comparison for storage required for ciphertext is also done and represented in Fig. 6. It can be concluded from the Fog. 6 that the amount of storage required to store ciphertext generated by proposed method is very much less as compared to traditional CPABE.

As hierarchical access structure is used to all messages are encrypted with hierarchical access tree and hence only one ciphertext is obtained. In case of traditional scheme the separate access structure is used for encrypting respective message and hence separate ciphertext is obtained. Due to this the time required to encrypt all messages is less as compared to traditional system. Also while decrypting the proposed method takes less time as only partial access structure is to be matched and the respective message is obtained. Thus the performance of proposed system is better as compared to traditional scheme.

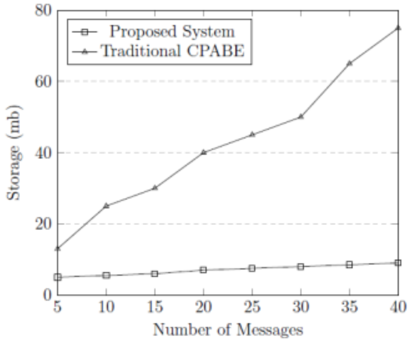

Fig. 5 Comparison of Storage required for Ciphertext

5. Conclusion

The paper represents the trust and hierarchical access structure based scheme for the cloud environment. In order to ensure that the data is secured in cloud environment, it is necessary to allow only authorized access to the data. Also establishing trusted relationship between users and service provides is of prime importance. Hence the paper presents the trust evaluation scheme that utilizes TOPSIS method, for service providers and for users. The trust levels are assigned to the service providers by considering performance parameters. Similarly the uses are evaluated on basis of their behaviour and respective trust levels are assigned to them. The results shows that the proposed trust evaluation scheme is more accurate that the existing ones. The other major objective of paper is to apply hierarchical access structure while encrypting messages. The hierarchical approach eliminates need of generation of many different access structures and ciphertexts. The proposed method allows decryption of messages based on fulfilment of access structure. The proposed scheme has better performance as compared to traditional system in terms of encryption time and decryption time. Also, it requires less amount of storage for ciphertexts as it eliminated need of multiple ciphertexts. Thus, the proposed scheme is computationally efficient that the traditional scheme. The scheme can be further improved by considering different threshold gates in access structure. Also different other parameters for computing trust levels can be applied to improve performance.

Paper2

ORIGINALITY REPORT

6%
SIMILARITY INDEX

PRIMARY SOURCES

1	D.S. Guru. "Finite Automata Inspired Model for Dominant Point Detection: A Non-Parametric Approach", 2007 International Conference on Computing Theory and Applications (ICCTA 07), 03/2007 Crossref	30 words — 1%
2	Calvin Newport. "Provably secure ciphertext policy ABE", Proceedings of the 14th ACM conference on Computer and communications security - CCS 07 CCS 07, 2007 Crossref	24 words — < 1%
3	"Algorithms and Architectures for Parallel Processing", Springer Science and Business Media LLC, 2015 Crossref	22 words — < 1%
4	Faramak Zandi. "A multi-attribute group decision support system for information technology project selection", International Journal of Business Information Systems, 2010 Crossref	19 words — < 1%
5	Lecture Notes in Computer Science, 2014. Crossref	16 words — < 1%
6	www.hindawi.com Internet	15 words — < 1%

7	www.mdpi.com Internet	15 words — < 1%
8	Jinguang Han, Willy Susilo, Yi Mu, Jun Yan. "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems, 2012 Crossref	13 words — < 1%
9	docplayer.net Internet	13 words — < 1%
10	Zaobo He, Zhipeng Cai, Qilong Han, Weitian Tong, Limin Sun, Yingshu Li. "An energy efficient privacy-preserving content sharing scheme in mobile social networks", Personal and Ubiquitous Computing, 2016 Crossref	12 words — < 1%
11	www.springerprofessional.de Internet	11 words — < 1%
12	"Computer Security – ESORICS 2019", Springer Science and Business Media LLC, 2019 Crossref	9 words — < 1%
13	Xiao, Min, Mingxin Wang, Xuejiao Liu, and Junmei Sun. "Efficient distributed access control for big data in clouds", 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2015. Crossref	9 words — < 1%
14	mafiadoc.com Internet	9 words — < 1%
15	www.inderscience.com Internet	9 words — < 1%

16	"Enhancing the Internet with the CONVERGENCE System", Springer Science and Business Media LLC, 2014 Crossref	8 words — < 1%
17	Balasubramaniam, P.. "Elliptic curve scalar multiplication algorithm using complementary recoding", Applied Mathematics and Computation, 20070701 Crossref	8 words — < 1%
18	Dhruti Sharma, Devesh Jinwala. "ID-based secure key generation protocol", 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011), 2011 Crossref	8 words — < 1%
19	P. Shivakumara, G. Hemantha Kumar, H.S. Varsha, S. Rekha, M.R. Rashmi Nayaka. "A new moments based skew estimation technique using pixels in the word for binary document images", Eighth International Conference on Document Analysis and Recognition (ICDAR'05), 2005 Crossref	8 words — < 1%
20	Qin Liu, C. C. Tan, Jie Wu, Guojun Wang. "Reliable Re-Encryption in Unreliable Clouds", 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, 2011 Crossref	8 words — < 1%
21	Zeeshan Pervez, Asad Masood Khattak, Sungyoung Lee, Young-Koo Lee. "SAPDS: self-healing attribute-based privacy aware data sharing in cloud", The Journal of Supercomputing, 2012 Crossref	8 words — < 1%
22	worldwidescience.org Internet	8 words — < 1%

23	www.scpe.org Internet	8 words — < 1%
24	Liu, Xuejiao, Yingjie Xia, Wenzhi Chen, Yang Xiang, Mohammad Mehedi Hassan, and Abdulhameed Alelaiwi. "SEMD: Secure and efficient message dissemination with policy enforcement in VANET", Journal of Computer and System Sciences, 2016. Crossref	7 words — < 1%
25	Ibraheem, , N. K. Sharma, and P Tiwari. "Compatibility of network matrices and possible application in power system", 2010 Joint International Conference on Power Electronics Drives and Energy Systems & 2010 Power India, 2010. Crossref	6 words — < 1%
26	ink.library.smu.edu.sg Internet	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		