Security and Privacy Preserving by using Two Layer Encryption Process in Public Cloud

Uma B. Ajantiwale, Prof. R. R. Badre

***Abstract*—Thetraditional and Single Layer Encryption (SLE) approaches incur high communication and computational cost to manage key and encryption whenever user credentials change. So to overcome this problem, the Two Layer Encryption (TLE) process is proposed. In this, the TLE process solve that problem by usingthe access control enforcement responsibilities as possible to the cloud while minimizing the information revelation risks due to machinating users and cloud. Under this approach, the data owner performs the coarse-grained encryption and the cloud performs the fine grained encryption. A challenging issue of the TLE process is to decompose the access control policy into two sub ACPs so that the owner has to handle a minimum number of attribute condition while hiding the content from the cloud. The policy decomposition problem is the NP-Complete problem and provided approximation algorithm. The system assures about the confidentiality of the data and preserves the privacy of user from the cloud while delegating most of the access control enforcement to the cloud.**

***Index Terms*–Security, Privacy, Confidentiality Identity, Cloud Computing, Access Control, Policy Decomposition, Encryption.**

I. INTRODUCTION

Today, security, privacy and confidentiality are the major concerns in the cloud technology for data storage. To reduce these concerns, encryption is the way. But, encryption only assures the confidentiality of the data against the cloud, so the use of conventional encryption approach is not sufficient to support the application of fine-grained [10] organization access control policies (ACP). Today many organizations have ACPs regulating, it decides which users can access which type of data. These ACPs are stated in terms of the properties of the users, raised as identity attributes, using access control languages such as a XACML[3], [5]. The identity attributes encode private information and thus should strongly protect from the cloud, very much as data themselves.

In the traditional approach, group of data itemsare based on the ACPs and encrypted with the different symmetric keys. Users which are present in group, only those have given a key to access that data item. Such approaches consist of several limitations:

1. The data owner does not keep copy of the data, whenever user dynamics changes. If the data owner wants to download the data, decrypt the data, and changed it after that re-encrypt it with new key and then upload it on the cloud. So the user dynamic changes refer to the operation of adding and revoking user. But this process must be applied to all data items encrypted with same key. If the data set is large then it is not efficient for re-encryption process.
2. Data owner needs to establish private communication channels with the users, when data owner wants to generate the new key for user.
3. The user's identityattributes is not taken into account for the privacy. Therefore, the cloud can be learning sensitive information about the user and the organization.
4. They are not either able or efficient in supporting fine-grained access control policies.

Recently proposed approach is based on the broadcast key management schemes, which is called as Single Layer Encryption (SLE) [6] process. This process addresses the above some limitations. So to overcome these limitations, the Two Layer Encryption (TLE) [1],[2],[4] process is proposed. The approach is based on the two layer encryption applied to each data item then upload to the cloud. In the two layer encryption process, firstly the data owner can encrypt the data that process called as Coarse-grained encryption. On the cloud side encrypted data can be re-encrypted and uploadedon to the cloud that process called as a Fine-grained encryption. The TLE process is not new, however the way of TLE (Coarse-grained and fine-grained) is novel and provide better solution than existing process.

In the TLE, the main challenge is decomposing the ACPs, so that fine-grained attribute based access control (ABAC) enforcement can delegate to the cloud. While at the same time the privacy of the identity attributes of the users and confidentiality of the data are assured.

The rest of the paper is organized as follows:- Section II describes the related work, section III describes proposed work, then section IV conclude the process.

II. RELATED WORK

Privacy Preserving Access Control – It is very difficult to manage database system in house especially for small or medium organizations. For those organizations, Data-as-a-Service (DaaS) [7] has provided the alternative solution in the cloud, which is very flexible, reliable, easy and economical to operate. However, security and privacy are the major issues for the data storage in the cloud and access via internet have been major issues for many organizations. The data and the human resources are the most important part of any

ISSN:2278 – 7798

organization. Hence, they should strongly protect. In this method, identifying the challenging issues in securing DaaS model so that they proposed a system called as a Cloud Mask that puts the foundation for organization to take all types of the benefits of hosting their data in the cloud.At the same time, DaaS has also supported for fine-grained access control for sharing the data hosted in the cloud.

Broadcast Group Key Management-The main problem in the public cloud is how to selectively share the documents, which is based on fine-grained ABAC policies. In this approach, the documents must satisfy different policies for the encryption with different keys using public key cryptosystem called as an Attribute based Encryption (ABE) and Proxy Encryption (PRE). However, this approach consists of some limitations: it incurs high communication and computation cost to keep multiple numbers of encrypted copies of the some documents. So to overcome this problem, a new key management schemes is proposed called as Broadcast Group Key Management (BGKM) [7], [8], [11], [12], [13], [14] and after that they can be provided a secure construction of a BGKM scheme called as an Access Control Vector-BGKM (ACV-BGKM). This idea is to provide some secrets to user which is based on their identity attribute and latterly they will allow them to derive actual symmetric key based on their secrets and some their public information. The advantage of BGKM scheme is that adding/revoking users or updating ACPs can be performed easily by updating only some public information. Using BGKM construct, an efficient approach is proposed for fine-grained encryption based on the access control for storing the documents in untrusted cloud.

Over Encryption: Management of access Control evolution of out-sourced data- In this, two layer encryption (TLE) [9] method is proposed. This method is enforced on data. The inner layer is enforced by the owner for providing initial protection and the outer layer is also enforced by the server to reflect the policy modification. The TLE method provides both the efficient and robust solution. A model is proposed an algorithm for the management of the two layersencryption and an analysis to identify there counteracts.There is an emerging trend towards scenarios where resource management is outsourced to an external service providing storage capabilities and high-bandwidth distribution channels.

III. PROPOSED WORK

The approach is based on the two layer encryption process is applied to each data items uploaded to the cloud. In the TLE approach, data owner can perform first encryption which is called as the coarse-grained encryption in order to assure the confidentiality of the data from the cloud. Then cloud can perform the second re-encryption on the encrypted data item that process called as the fine grained encryption. The two layer encryption is not new, but the way of representation of this TLE process is new. The coarse grained and fine grained process is new and provides a better solution than existing solution. The TLE process consists of the four entities Owner, User, Identity Provider (Idp), and Cloud as shown in fig. 1. This TLE process reduces the load of the data owner and delegate as much access control enforcement duties as possible to the cloud. Mainly, it overcomes the traditional approaches so it provides a best way to handle the data updates and user dynamics changes.

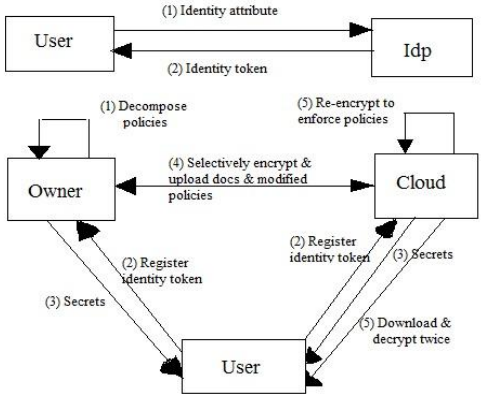

Fig. 1: Two Layer Encryption Architecture

Algorithm-

1. *Gen-Graph Algorithm-*

C = φ
forEach $ACP_i \in ACPB$, i = 1 to $N_p$do
    $ACP_i' \leftarrow$ Convert ACP_i to DNF
    forEach conjunctive term c of ACP'_ido
        Add c to C
    end for
end for
//Represent the conditions as a graph
G = (E, V), E = φ, V = φ
forEach conjunctive term ci ∈ C, i = 1 to $N_c$do
    Create vertex v, if v not belongs to V, for each AC in ci
    Add an edge ei between vi and each vertex already added for ci
end for
Return G.

Graph generation algorithm takes the Access Control Policy) as the input and converts each ACP into Disjunctive Normal Form (DNF). Then each conjunctive term which is present in ACP that will be added into the set C. For each attribute condition (AC) in each conjunctive term in C set, it generates a new vertex in G and adds edges between the vertices corresponding to the same conjunctive term. Depending on the ACPs, the algorithm can create a graph G with multiple disconnected subgraphs or connected subgraghs.

ISSN:2278 – 7798

Access Control Policy Based (ACPB)-
(“role = rec” ∨(“role = nur” ∧“type ≥ junior”), CI)
(“role = cas” ∨“role = pha”, BI)
(“role = doc” ∧“ip = 2-out-4”, CR)
((“role = doc” ∧“ip = 2-out-4”) ∨“role = pha”, TR)
((“role = doc” ∧“ip = 2-out-4”) ∨(“role = nur” ∧“yos≥ 5”) ∨“role = pha”, MR)
((“role = nur” ∧“type ≥ junior”) ∨(“role = dat” ∧“type ≥ junior”) ∨(“role = doc” ∧“yos≥ 2”), LR)
((“role = nur” ∧“type = senior”) ∨(“role = dat” ∧“yos≥ 4”), PE)

Output of the Gen-Graph algorithm-

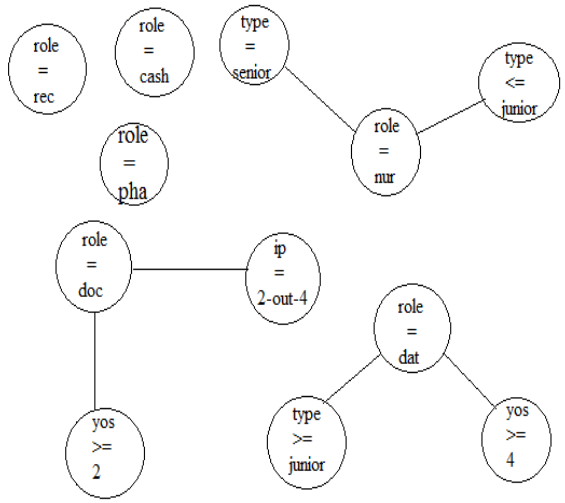

Fig. 2: The example of graph

2. Random Edge Algorithm-

G = GEN-GRAPH(ACPB)
ACC = φ
forEach disconnected subgraph$G_i = (V_i,E_i)$ of G do
    if|Vi| == 1 then
    Add AC_i corresponding to the vertex to ACC
    else
    whileE_i not equal to φ do
        Select a random edge (u, v) of E_i
        Add the attribute conditions AC_u and AC_v corresponding to {u, v} to ACC.
        Remove from E_i every edge incident oneither u or v
    end while
    end if
end for
Return ACC.

The Random cover algorithm takes the ACPs as the input and generates output a near optimal ACC(attribute condition cover). Gen-graph algorithm calls this algorithm to generate disconnected or connected graph as shown in above algorithm. Through each disconnected graph Gi of G, it finds the near optimal ACC and adds to the ACC’. If the graph is connected then algorithm is selected any random edge is considered, then all edges are removed from Gi. The algorithm continues until all edges are removed from each Gi.

The output of the Random policy algorithm-
It gives the AC cover ACC = {“role = cas”, “role = eac”, “role = doc”, “role = pha”, “yos ≥ 2”, “role = nur”, “role = dat”}. The optimal AC cover ACC = {“role = cas”, “role = rec”, “role = doc”, “role = pha”, “role = dat”, “role = nur”}.

3. *Policy Decomposition-*

$ACPB_{Owner}$ = φ
$ACPB_{Cloud}$ = φ
forEach ACP_i in ACPB do
    Convert ACP_i to DNF
    ACP_i(owner) = φ
    ACP_i(cloud) = φ
    ifOnly one conjunctive term then
    Decompose the conjunctive term c into c_1 andc2 such that ACs in c1 ∈ ACC, ACs in c2 not belongs to ACC and c = c1∧ c2
        ACP_i(owner) = c1
        ACP_i(cloud) = c2
else if At most one term has more than one AC then
    forEach single AC term c of ACP'_ido
    ACP_i(owner) ∨ = c
    ACP_i(cloud) ∨ = c
    end for
Decompose the multi AC term c into c1 and c2such that ACs in c1 ∈ ACC, ACs in c2 not belongs to ACCand c = c1 ∧ c2
    ACP_i(owner) ∨= c1
    ACP_i(cloud) ∨= c2
else
    forEach conjunctive term c of ACP'_i**do**
    Decompose c into c1 and c2 such that ACsin c1 ∈ ACC, ACs in c2 not belongs to ACC and c = c1 ∧ c2
        ACP_i(owner) ∨= c1
    end for
    ACP_i(cloud) = ACP_i
end if
Add ACP_i(owner) to $ACPB_{Owner}$
Add ACP_i(cloud) to $ACPB_{Cloud}$
end for
Return $ACPB_{Owner}$ and $ACPB_{Cloud}$

The policy decomposition is used to decompose the ACPs into two sub ACPs. The owner manages only those

ISSN:2278 – 7798

attribute conditions which are in the ACC. The cloud can be handling the remaining set of attribute condition, which is in ACB or in AC. The algorithm is showed how the ACPs are decomposed into two sub Access Control Policies based on the AC in ACC. The algorithm is taken the input from ACPB and produced the two sets of ACPs which are$ACPB_{owner}$ and $ACPB_{cloud}$ that are to be enforced at the owner side and the cloud side respectively. The algorithm converts each conjunctive term in two parts such that one conjunctive term has only those ACs which belongs to ACC and the other term may or may not belong to ACC. It is easily shown that the policy decomposition is consistent. That is, the conjunctive of corresponding sub ACPs in $ACPB_{ower}$ and $ACPB_{cloud}$ generates an original ACP in ACPB.

The output of the policy decomposition algorithm, the sub ACPs that owners enforce look like follows-

(“role = rec” ∨“role = nur” , CI)
(“role = cas” ∨“role = pha”, BI)
(“role = doc”, CR)
(“role = doc” ∨“role = pha”, TR)
(“role = doc” ∨“role = nur” ∨“role = pha”, MR)
(“role = nur” ∨“role = dat” ∨“role = doc”, LR)
(“role = nur” ∨“role = dat”, PE).

The sub ACPs that cloud enforces look like as follows-
(“role = rec” ∨“type ≥ junior”, CI)
(“role = cas” ∨“role = pha”, BI)
(“ip = 2-out-4”, CR)
(“ip = 2-out-4” ∨“role = pha”, TR)
((“role = doc” ∧“ip = 2-out-4”) ∨(“role = nur” ∧“yos≥ 5”) ∨“role = pha”, MR)
((“role = nur” ∧“type ≥ junior”) ∨(“role = dat” ∧“type ≥ junior”) ∨(“role = doc” ∧“yos≥ 2”), LR)
((“role = nur” ∧“type = senior”) ∨(“role = dat” ∧“yos≥ 4”), PE)

Modules-

1. Identity Token Issuance

Identity Provideris called as trusted third parties that issue identity tokens to Users based on their identity attributes. After the issuing identity token, it goes on offline mode.

2. *Policy Decomposition-*

The Owner can be decomposed each ACP into two sub ACPs using the policy decomposition algorithm such that the owner can be enforced the minimum number of attribute to assure the confidentiality of data from the cloud. The algorithm generates two sets of sub ACPs $ACPB_{owner}$and $ACPB_{cloud}$. The owner can enforce the confidentiality related with sub ACPs in $ACPB_{owner}$ and the cloud can be enforced the remaining sub ACPs into the $ACPB_{cloud}$.

3. Identity Token Registration-

Using the user credential, identity token is generated. Through this Identity Token (IT), secrets can be obtained to decrypt the data for the accessing that data.

4. *Data encryption and upload-*

In the TLE process, data is encrypted two times, firstly at the owner side and secondly at the cloud side. The owner can be encrypted the data based on the sub ACPs which present in $ACPB_{owner}$ and uploads them to the cloud. Then cloud re-encrypts the encrypted data based on remaining sub ACPs which is present in the $ACPB_{cloud}$. For the generation of symmetric key, both parties can be executed Advance Encryption Standard algorithm individually.

5. Download and Decryption algorithm-

Users download the encrypted data from the cloud and then decrypt the encrypted data two times to access that data. First, the cloud can be generated public information tuple, then it can be used to derive the out layer encryption key and after that the owner generates public information tuple is used to drive the inner layer encryption key using the AES algorithm. These two keys are allowed a user to decrypt a data item only if the user satisfies the original ACPs applied to the data item.

6. Authentication Server-

Kerberos protocol is used for authenticating users by their login credentials. Kerberos is one of the types of Single Sign-On (SSO) protocol to provide Ticket passing and validation of user login. Kerberos will validate the user login, if user is authenticated it will generate the login ticket available for some instance of time and send tickets to application and user browser, then user login will be done by forwarding user authentication ticket to application and signature checking of that ticket. To develop Kerberos Protocol, SHA-1 algorithm is used to generate and verify user login ticket.

IV. RESULT ANALYSIS

In the previous method, ABGKM Algorithm is used to encrypt and decrypt the data items. But in this Advanced Encryption Standard (AES) Algorithm is used for encryption and decryption purpose. The AES algorithm takes the less time to encrypt or decrypt the data items and provide more security also as compared to ABGKM algorithm. Fig. 3 and 4 show exact difference between both algorithms.

The average time spent to executethe AB-GKM::KeyGen with SLE and TLE approaches for different group sizes. The number of attribute conditions to 100 set and the maximum number of attribute conditions per policy is dynamic. SLE approach utilizes the greedy algorithm to find the attribute condition cover. As seen in the Fig 5, the running time at the Owner in the SLE approach is higher since the Owner has to enforce all the attribute conditions. Since the TLE approach utilizes the random cover algorithm and divides the

ISSN:2278 – 7798

enforcement cost between theOwner and the Cloud, the running time at the Owner is lower compared to the SLE approach. The running time at the Cloud in the TLE approach is higher than that at the Owner since the Cloud performs fine grained encryption whereas the Owner only performs coarse grained encryption. Through this, computation and communication cost is also reduced.

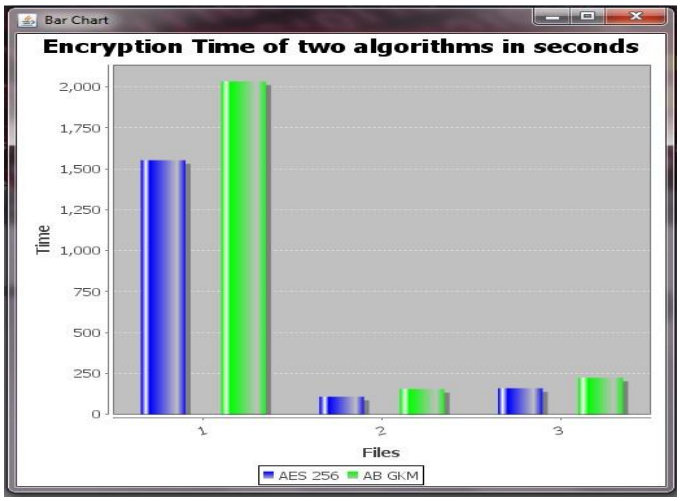

Fig. 3: Difference between AES and ABGKM Algorithm for encrypting the data items.

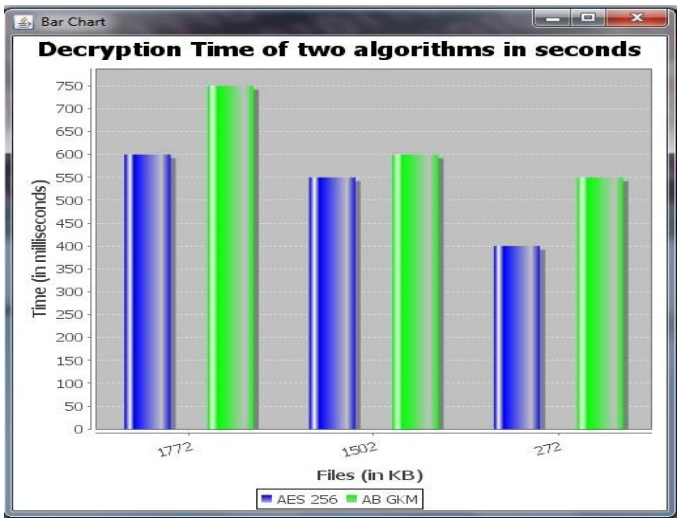

Fig. 4: Difference between AES and ABGKM Algorithm for decrypting the data items.

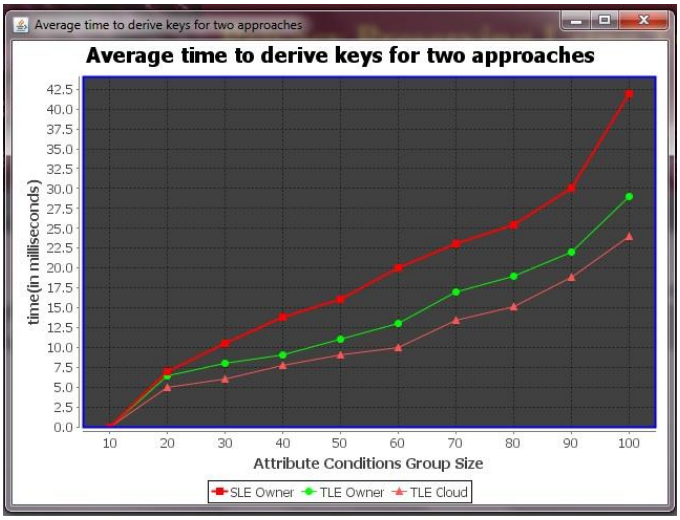

Fig. 5 Average time to derive keys for the two approaches

V. CONCLUSION

The traditional and SLE approaches incur high communication and computational cost to manage key and encryption whenever user credentials changes. In this, the two layer encryption process is used to overcome thisproblem by using the access control enforcement responsibilities as possible to the cloud. A challenging issue of the TLE process is to decompose the access control policy into two sub ACPs so that the owner has to handle a minimum number of attribute condition while hiding the content from the cloud. The policy decomposition problem is the NP-Complete problem and provided approximation algorithm.

ACKNOWLEDGEMENT

I express true sense of gratitude towards my project guide **Prof. Ranjana Badre.**, of computer department for her invaluable co-operation and guidance that she gave me throughout my research. I specially thank to our **P.G coordinator Prof. R. M. Gaudar**for inspiring me and providing me all the lab facilities, which made this research work very convenient and easy. I would also like to express my appreciation and thanks to our HOD **Prof.Uma Nagaraj**andprincipal**Dr. Y. J. Bhalerao**and all my friends who knowingly or unknowingly have assisted me throughout my hard work.

REFERENCES

[1] M. Nabeel and E. Bertino, “Privacy Preserving delegated access control on Public Clouds”, IEEE Transactions on Knowledge and Data Engineering, 2013.

[2] Uma B. Ajantiwale and Prof. Ranjana Badre, “Survey on Two Layer Encryption System”, IJIRCCE, Nov 2014.

[3] E. Bertino and E. Ferrari, “Secure and selective disseminationof XML documents,” *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 3,pp. 290–331, 2002.

ISSN:2278 – 7798

[4] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in EEEInternational Conference on Information Reuse and Integration(IRI), 2012.
[5] Miklau and D. Suciu, "Controlling access to published data using cryptography," Proceedings of the29th international conference on Very largedata bases. VLDB Endowment, pp. 898–909, 2003.
[6] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacy preserving approach to policy-based content dissemination," Proceedings of the IEEE26th InternationalConference on Data Engineering, 2010.
[7] M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, "Towards privacy preserving access control in the cloud," in Proceedings ofthe 7th International Conference on CollaborativeComputing: Networking, Applications and Worksharing, ser. CollaborateCom. 11 pp. 172–180, 2011.
[8] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Transactionson Knowledge andData Engineering, 2012.
[9] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution onoutsourced data," in Proceedings of the33rd International Conference on Very Large Data Bases, VLDB Endowment, pp. 123–134, 2007.
[10] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of the13th ACM conference on Computerand communications security. New York, NY, USA: ACM, pp. 89–98, 2006.
[11] Y. Challal and H. Seba. "Group key management protocol: A novel taxonomy". International Journal of Information Technology, 2(2):105-118, 2006.
[12] Chiou and W. Chen "Secure Broadcasting using the secure lock". Software Engineering IEEE Transaction on, 15(8):929-934, Aug 1989.
[13] X. Zou, Y. Dai and E. Bertino. "A practical and flexible key management mechanism for trusted collaborative computing". INFOCOM the 27thConference on Computer Communication IEEE, pages 538-546, April 2008.
[14] N. Shang, M. Nabeel, F. Paci and E. Bertino, "A privacy-preserving approach to policy-based content dissemination". In ICDE Proceedings ofthe IEEE 26th International Conference on Data Engineering 2010.
[15] A .Reddy, GudivadaLokesh and N. Vikram "Privacy Preserving Delegated Access Control in Public Clouds", International Journal ofComputer Science Trends and Tech (IJCST)- Vol. 2 Issue 4, July Aug 2014.

Uma B. Ajantiwale received B.E. degree in Information Technology from Nagpur University in 2013 and pursuing her M.E. degree in Computer Engineering in the Department of Computer Engineering in MIT Academy of Engineering, Pune.

Prof. R.R. Badre received her M.E. degree in Computer Science and Engineering from Shivaji University, Kolhapur. She is currently working as an Associate Professor in the Department of Computer Engineering in MIT Academy of Engineering, Pune. She has published more than 12 papersin both International journals and conferences. She is also a member in Indian Society of Technical Education.

ISSN:2278 – 7798