Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

An Efficient and Secured Data Access Control with Two Layer Decentralized Dynamic Broadcast Encryption

S.MUTHUKUMAR
PG Scholar
SNS College of Technology, Coimbatore. India

C.VIMALARANI
Assistant Professor - CSE
SNS College of Technology, Coimbatore. India.

Abstract— ***Cloud computing is a buzz word which means that accessing and storing of data and programs over the Internet instead of your computer's hard drive. Security and privacy represent major concerns in the adoption of cloud technologies for data storage. An approach to mitigate these concerns is the use of fine grained access control encryption. But in this approach Data owners thus incur high communication and computation costs. To overcome these problem data owner performs a coarse-grained broad cast encryption along with two layer process, whereas the cloud performs a fine-grained encryption on top of the owner encrypted data. A challenging issue is how to decompose access control policies (ACPs) such that the two layer encryption can be performed. To overcome these problem proposed go a step further in the decentralization process in two layer broadcast encryption schema, by removing the group manager initial setup of the group, as well as the addition of further members to the system, does not require any central authority. Our construction makes black-box use of well-known primitives and can be considered as an extension to the subset-cover framework. It allows for efficient concrete instantiations, with parameter sizes that match those of the subset-cover constructions, while at the same time achieving the highest security level in the standard model .It utilize an efficient decentralized group key management scheme that supports expressive ACPs. Our system assures the confidentiality of the data and preserves the privacy of users from the cloud while delegating most of the access control enforcement to the cloud.***

Keywords— ***Delegation, privacy, access control, security, policy, Cloud Computing and decentralized Dynamic Broadcast Encryption, Two layer encryption.***

I. INTRODUCTION

In typical access control models, the set of access rights a user gets is predetermined. Predetermining a user's access rights is equivalent to anticipating possible usages of the system by that user. There are two ways to assign access rights. First, a system administrator acts every time a user needs an access right. Secondly, a user gets the right from another user who already possesses it. The latter approach is called delegation.

Delegation brings flexibility to access control models. Zhang et al. [1] identify three cases when delegation is necessary. In the first, an individual is absent from their job and so, someone else should carry out the tasks. Secondly, delegation is allowed to decentralize the authority. Having one system administrator who assigns access rights to all the users in the system would decrease efficiency.

To study privacy preserving delegation, need an environment where data providers provide privacy policies for their data. The policies would state who can use the data and how the data should be used. The access control models in such environments control data accesses based on the privacy policies. These are known as privacy preserving access control models. Several models have been proposed [2-3] in the literature. One of our contributions is to define a privacy model that allows a data provider to set privacy policies for different organizations accessing their data.

Broadcast encryption is a scheme that allows a sender to send a cipher text to some designated groups whose members of the group can decrypt it with his or her private key. However, nobody outside the group can decrypt the message. The broadcast encryption can be divided into two categories from a relation of receivers. In the first category, a sender can randomly designate several receivers. Users in this category may be no relation between each other. For the second category, a sender can encrypt a message to a designated group in which each user in the group can use his private key independently to decrypt the cipher text. Users can contact with other users in the group and all users in the group are listening on a broadcast channel. Usually the first category has lots of advantages. It is more flexible than the second category and sender can randomly designated a subset of receivers. However, these advantages make the first category much more complicated. It is very difficult to make the scheme satisfy so many advantages while keep the cipher text and keys constant size. For a network like a mobile ad hoc network, the complex in computation and the need for large memory make it inefficient.

Recently proposed approaches based on broadcast key management schemes [4] address some of the above limitations. Then refer to these approaches as single layer encryption (SLE) approaches, since, like previous approaches, they require the data owner to enforce access control through encryption performed at the data owner. However, unlike previous approaches, SLE assures the privacy of the users and supports fine-grained ACPs.

To overcome the major problem of SLE proposes a new approach to address this shortcoming. The approach is based on two layers of encryption applied to each data item uploaded to the cloud. Under this approach, referred to as two layer encryption (TLE), the data owner performs a coarse grained encryption over the data in order to assure the confidentiality of the data from the cloud. Then the cloud performs fine grained encryption over the encrypted data provided by the data owner based on the ACPs provided by the data owner. But the two layer encryption schema the broadcast encryption schema the centralized group manager is either involved once only, at the setup phase, in static schemes, or at any time a new member wants to join the system, in dynamic schemes [5]. The latter dynamic situation is the most realistic, but makes the group manager quite sensitive, for both security and availability. Our goal is to get rid of such a centralized system.

The proposed privacy model is used in conjunction with the access control model to create privacy-aware access rights i.e., the rights containing constraints that specify the valid use of data along with two layer dynamic decentralized broadcast encryption schema, it does not requires any specific centralized authority every time to access or policy in the cloud computing group key managements process. Data users assigned to these rights use data according to the constraints. Based on these foundations, propose a delegation two layer dynamic decentralized model where access rights to a data item can be delegated only if it is allowed by the data item's privacy policies. Since the delegated rights contain privacy constraints, the users who receive the rights are bound by the privacy constraints when they use the data. It also investigate prohibiting certain delegation operations to maintain the access control model's security.

II. Existing System

The existing system, represents several encryption based access control policies over the data with encrypted group of different symmetric key controls [13]. The keys are given only to the user data that which are accessible and links are provided to reduce the number of keys need to distributed over the user have been implemented to utilize hierarchical and other functions on the data items. By implementing these approach some disadvantages has been involved, the keys issued to the user can be established by data owner through the private communication channel with the users. The cloud data owner does not keeps the copy of the data when the user dynamic changes. The data owner process the download of data, upload of data, decrypt and re-encrypt of data. These process can be applied to all cloud data items with the same encrypted key. When the data set to be re-encrypted is large with this method. The identity attributes of the user are not taken in account of privacy. The enforcement of all ACPs by the existing system encryption, the owner requires to ratify and revoke the user initially and subsequently. By implementing these encryption scheme the activities performed at the owner incurs high computational cost and communication.

III. Proposed System

In the proposed system, we implement the two layer encryption [6] scheme over the untrusted public cloud. The two layer enforcement reduce the load over the owner and delegates the enforcement of access control over the cloud. The system gives a better way for various updates, user location and modification of data, also includes an additional phase when compared to the existing system. The decomposition and splitting of the data to store across the different clouds and it is finally retrieved with the help of the keys provided by the provider to the users. The cryptographic technique scheme used in the proposed system possess symmetric key for both secure encryption and decryption. The group key management over the data owner and cloud service, the actual key are not provided to the user. But it distribute one or more temporary keys that which allow to retrieve the actual symmetric key for the decryption of data from the public cloud. We move to the decentralized dynamic broadcast scheme to store data over cloud with the dynamic changes of access control mechanism rights, that the authorized user with the valid key only able encrypt and decrypt the data that which stored in the untrusted cloud environment.

IV. Two Layer Decentralized Dynamic Encryption

The two layer encryption approach implements six phases over secure encrypt and decrypt of data. The approach consists of four entities Data Owner, Authorized User, Identity Provider and Cloud.

A. Identity Token Providence: IdPs issue identity tokens to users based on the identity attribute over the trusted third parties.

B. Policy Decomposition: The owner decompose each ACP into two sub ACPs such that the owner assure confidentiality of data with the minimum number of attributes. The owner enforce the confidentiality related to the sub ACPs over the owner and the remaining sub ACPs enforces the cloud.

C. Identity Token Registration: The user register their identity tokens to decrypt the data. User register those identity tokens related to the owner's sub ACPs and the remaining identity tokens are registered on the cloud in privacy preserving manner. In this phase the owner keeps one set and another set is provided to the cloud. The two sets used to prevent the cloud from the decrypting owner encrypted data.

D. Data Encryption and Uploading: The owner encrypts the data which based on the sub ACPs and uploads the data along with the corresponding tuples to the cloud. The cloud encrypts the data again based on the sub ACPs. The keys at the cloud takes secret issued to users and the sub ACPs given by the owner.

E. Data Downloading and Decryption: The download of encrypted data from cloud can be done by user and by using the derived keys the data decryption is processed. The decryption of data can be done twice by the user.

The main security goal of an encryption scheme (or an encapsulation scheme) is the in distinguishability of a challenge cipher text: at some point, the adversary thus gets a challenge (H, k_0, k_1) where H encapsulates either $k_0$or k_1

for a target set S chosen by the adversary. It has to guess which key is actually encapsulated. Of course, there are the natural restrictions, which are controlled granted the lists Q_c and Q_D:

- (S, H) has not been asked to the decapsulation oracle for a user u in S.
- None of the users in S have been corrupted.

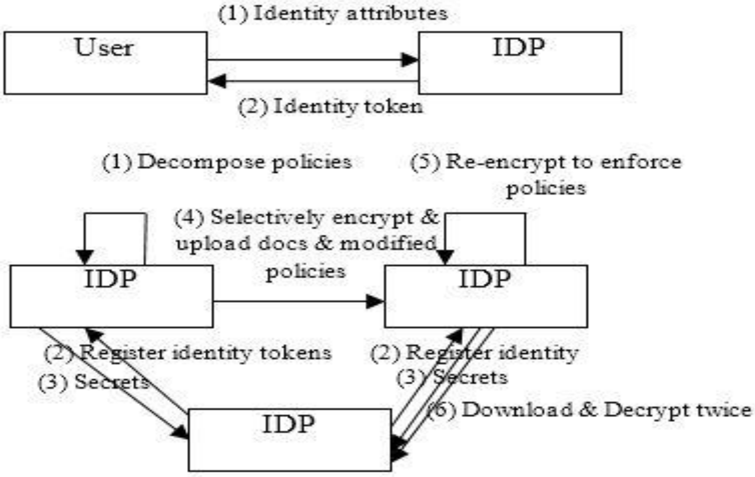
(1) Identity attributes
User
IDP
(2) Identity token
(1) Decompose policies
(5) Re-encrypt to enforce policies
(4) Selectively encrypt & upload docs & modified policies
IDP
IDP
(2) Register identity tokens
(3) Secrets
(2) Register identity
(3) Secrets
(6) Download & Decrypt twice
IDP

Figure 1 Two Layer Encryption

A dynamic broadcast[7] encapsulation scheme is $(t, N, q_c, q_D, \varepsilon)$ (security against adaptive corruption and chosen-cipher text attacks) if in the security game the advantage $Adv_{DB\mathcal{E}}^{ind-acca}(k, t, N, q_c, q_D, \varepsilon, ACP, PI)$ of any t-time adversary A creating at most the maximum group size N, $\boldsymbol{Usrj}$ corrupting at most q_c of them and asking for at most q_D decapsulation keys , is bounded by ε. Dynamic S-Subgroup Key Exchange Protocol: For a collection $S : N \rightarrow P(N)$ of subsets of the user set, where for any N, $S(N) \in P(N)$, a dynamic S-subgroup key exchange protocol SKE is a tuple of three algorithms and interactive protocols:

Setup$(1^k, N, N_a)$: It taking the security parameter 1^k, , the maximum group size N, and the number of attribute conditions N_a as input, initializes the system. It invokes DBE:Setup(ℓ, N) and ACV-DBGKM::Setup(ℓ, N)algorithms. $\boldsymbol{SecGen(param, \gamma)}$: The secret generation algorithm gives a Usrj , $1 \leq j \leq N$ a set of secrets for each commitment $comi \in \gamma, 1 \leq i \leq m$. It invokes DBE::GetSecGen algorithms. After the protocol run, it returns the public encryption key E_k and a list Reg of the registered users with additional public information. Each user $u \in Usrj(\gamma)$ eventually gets a secret decryption key dk_u.

KeyGen(ACP): The key generation algorithm takes the access control policy ACP as the input and outputs a symmetric key K, a set of public information tuples PI and an access tree T . It invokes $DBE::GetCover()$ and $ACV - DBGKM::KeyGen$ algorithms.

$\boldsymbol{Join}$ $(v, \{$ Usrj $(\boldsymbol{dk_{Usrj}})\}_{u \in Usrj(\gamma)}, \boldsymbol{reg\ GetCover}\ () : \boldsymbol{E_k})$ is an interactive protocol run between a user v and the set of users Usrj, described in Reg. Each user takes as input his secret key and/or some random coins, the list Reg, and the encryption key $\boldsymbol{E_k}$. After the protocol, Reg and $\boldsymbol{E_k}$are updated, and each user (including v) has a secret decryption key.

A subgroup key exchange schema is said to be $(t, N, q_t, PI, ACP, \varepsilon) - IND$ secure if in the security .The advantage $Adv_{SKE}^{ind}(k, t, N, q_T, \varepsilon, ACP, PI)$ of any time adversary $\mathcal{A}$ creating most N group size of users testing mode q_T key is bounded by ε

A decentralized dynamic broadcast encapsulation scheme is a tuple of five algorithms $DBE = (Setup; KeyGen; Join; Encaps; Decaps)$:

Setup$(1^k, N, N_a)$

1. Run $\mathcal{PKE}.Setup(1^k, N, N_a) to\ get\ para_{\mathcal{PKE}}$
2. Run $\mathcal{SKE}.Setup(1^k, N, N_a) to\ get\ para_{\mathcal{SKE}}$
3. Publish $param = (para_{\mathcal{PKE}}, para_{\mathcal{SKE}})$.

$KeyGen(param, Usrj_N)$ for some integer n :

1. Run $\mathcal{SKE}: KeyGen(para_{\mathcal{SKE}}, Usrj_N)$ to get Reg; Each user $u \in Usrj_N)$ gets as output of the protocol the proto-keys pt_S for all subsets S he belongs to according to SC_n The decryption keydk_u consists of all these pt_S.
2. He computes $(dk_s; ek_s)$ $\mathcal{PKE} : Keygen\ (param_{\mathcal{PKE}}; \mathcal{F}(pt_S))$ where we use the PRG to generate from the proto-key the random coins of the key generation algorithm;
3. All the encryption keys ek_s are published as E_k;
4. The decryption keys dk_s can be either stored in dku for users $u \in S$ or deleted since they can b Recomputed;

$Join$ $(v, \{$ Usrj $(dk_{Usrj})\}_{u \in Usrj(\gamma)}, reg, E_k)$

1. Run $\mathcal{SKE}: Join$ $(v, \{$ Usrj $(dk_{Usrj})\}_{u \in Usrj(\gamma)}, reg, E_k)$ to get the new Reg;

2. Each user u does as above to compute $dk_s;\ ek_s$ and dk_u. Note that granted the splitting properties, onlydk_s, and thus ek_s, for S that contain v are affected.

$Encaps(E_k;\ Reg;\ ACP, S, PI)$

1. From the target set S, generate the partition $\mathcal{L}$ with $S = \cup_{\mathcal{L}} S_i$
2. Generate a session key $\mathcal{K}_e$ and a MAC key $\mathcal{K}_m$;
3. For each subset $i \in \mathcal{L}$, generate $c_i = \mathcal{PKE}.Encrypt(ek_{si}, \mathcal{K}_e || \mathcal{K}_m);$
4. Compute $\sigma = \mathcal{MAC}.GenMac(\mathcal{K}_m, S||(c_i)_{i \in \mathcal{L}});$
5. Output $\mathcal{K}_e$ and $H = ((c_i)_{i \in \mathcal{L}}, \sigma)$

$\boldsymbol{decaps(dk_u;\ S, H, T, Reg, ACP, S)}$

1. If $Usrj \in S$ then there is a unique i such that $Usrj \in S_i$ and then $\boldsymbol{dk_u}$ allows to derive $\boldsymbol{dk = dk_{S_i}};$
2. Extract $(\mathcal{K}_e || \mathcal{K}_m) = \mathcal{PKE}.\mathrm{Decrypt}(\mathrm{dk}, \mathrm{c_i});$
3. check if σ is a valid MAC under Key $\mathcal{K}_m$;
4. In case of validity output $\mathcal{K}_e$ otherwise output $\perp$

The tree-based methods are special cases in the subset-cover framework, where the users are organized as leaves in a binary tree, and the subsets S_i can be described in terms of subtrees of this tree.

Complete sub tree: First review the static complete subtree (CS) (T) for cloud users { $Usrj_0, . Usrj_{N-1}\}$ .For simplicity assume that $N = 2^d$ but the description can be to generalized to any N Cloud user group size .All the users are leaves of the tree and can be seen as singletons $S_{2^d+i} = \{u_i\}$ for $i = 0, \dots, 2^d - 1$ then for $i = 2^d - 1$ to 1 , $S_i = S_{2i} U S_{2i+1}$ which contains all the leaves below for each cloud user with the index i .

Subset difference: The subset difference (SD) methods uses subsets $S_{i,j} = S_i / S_j$ where S_i, S_j are defined as in the CS methods and S_j is the subtree of S_i .All the set S_i from CS tree are also contained in the SD method because $S_i = S_{parent\ (i), sibiling(i)}; S_0$ included as a special set.

V. PERFORMANCE ANALYSIS

In this section first present experimental results concerning the policy decomposition algorithms. Then present an experimental comparison between the TLE and TLE Dynamic broadcast encryption approaches. Utilized the AB-GKM scheme with the subset cover optimization. Then used the complete subset algorithm introduced by Naor et. al. as the subset cover.

Figure 2 shows the size of the attribute condition cover, that is, the number of attribute conditions the data owner enforces, for systems having 100 attribute conditions as the number of attribute conditions per policy is increased. In all experiments, the Dynamic Subset-Cover algorithm performs better than greedy search cover algorithm, as the number of attribute conditions per policy increases; the size of the attribute condition cover also increases.

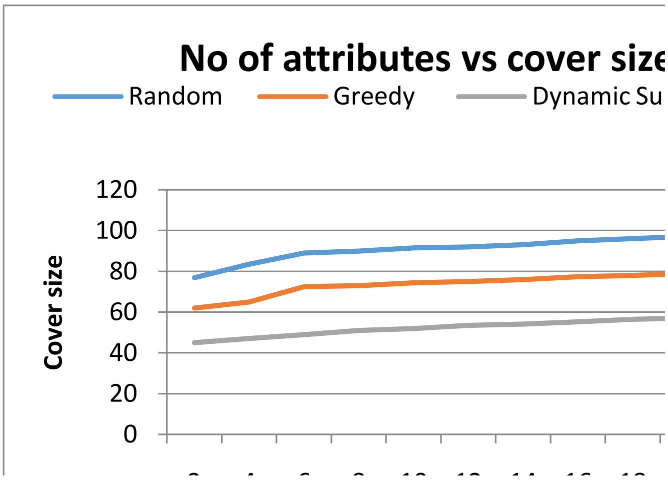

Figure 2: Size of ACCs for different number of ACs

Figure 3 reports the average time spent to execute the AB-GKM:: KeyGen with SLE and TLE ,TLE dynamic broadcast encryption approaches for different group sizes. Then set the number of attribute conditions to 1000 and the maximum number of attribute conditions per policy to 5. Then utilize the greedy algorithm to find the attribute condition cover. As seen in the diagram, 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 divides the enforcement cost between the Owners, the running time at the Owner is lower compared to the SLE approach. The running time at the TLE Dynamic broadcast encryption approach is higher than that at the Owner since the TLE, SLE fine grained encryption whereas the Owner only performs coarse grained encryption.

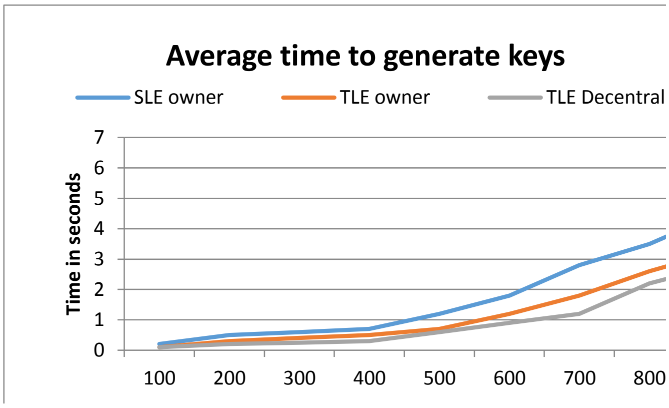

Figure 3: Average time to generate keys for the three approaches

VI. Conclusion

Current approaches to enforce ACPs on outsourced data using selective encryption require organizations to manage all keys and encryptions and upload the encrypted data to the remote storage. Such approaches incur high communication and computation cost to manage keys and encryptions whenever user credentials or organizational authorization policies/data change. In this paper, we proposed a two layer dynamic broadcast encryption based approach to solve this problem .The decentralized dynamic broadcast encryption and subgroup key exchange, a building block use in our construction that may be of independent interest by delegating as much of the access control enforcement responsibilities as possible to the Cloud while minimizing the information exposure risks due to colluding Usrs and Cloud. A key problem in this regard is how to decompose ACPs so that the Owner has to handle a minimum number of attribute conditions while hiding the content from the Cloud. As future work, plan to investigate the alternative choices for the TLE approach further. It also plans to further reduce the computational cost by exploiting partial relationships among ACPs.

Reference

[1] X. Zhang, S. Oh and R. Sandhu, “PBDM: a flexible delegation model n RBAC,” In proceedings of the eighth ACM symposium on Access control models and technologies (SACMAT), New York, NY, USA, pp. 149–157, 2003.

[2] M. Moniruzzaman, M.S. Ferdous and R. Hossain, “A study of privacy policy enforcement in access control models,” In proceedings of 13th International Conference on Computer and Information Technology (ICCIT). Dhaka, Bangladesh, pp. 352 – 357, 2010. DOI:10.1109/ICCITECHN.2010.5723883.

[3] M. Jafari, P. W. L. Fong, R. Safavi-Naini, K. Barker, and N. P. Sheppard, “Towards Defining Semantic Foundations for Purpose- Based Privacy Policies,” In proceedings of the First ACM Conference on Data and Application Security and Privacy (CODASPY), San Antonio, Taxas, USA, 213-224, 2011.

[4] N. Shang, M. Nabeel, F. Paci, and E. Bertino, “A privacy-preserving approach to policy-based content dissemination,” in ICDE ’10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

[5] Thuraisingham, “Towards privacy preserving access control in the cloud,” in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work-sharing, ser. Collaborate Com ’11, 2011, pp. 172–180.

[6] M.Nabeel, N.Shang, and E.Bertino, “Privacy preserving policy based content sharing in public clouds,” IEEE Transactions on Knowledge and Data Engineering, 2012.

[7] Cecile Delerablee, Pascal Paillier, and David Point cheval. Fully collusion secure dynamic broadcast encryption with constant-size cipher texts or decryption keys. In T. Takagi et al., editor, Pairing 2007, volume 4575 of LNCS, pages 39-59. Springer, 2007.

[8] K. Barker, M. Askari, M. Banerjee, K. Ghazinour, B. Mackas, M. Majedi, S. Pun and A. Williams, “A data privacy taxonomy,” In proceedings of the 26th British National Conference on Databases. LNCS. vol. 5588, pp. 42-54, 2009.

[9] Ayesha Malik, Muhammed Mohsin Nazir,”Security Framework for Cloud computing environment: Review’, Journal of emerging Trends in computing and information sciences”, Vol;3, No:3, March 2012, ISSN 2079-8407.

[10] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, “A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security”, Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.

[11] Mariana Raykova, Hang Zhao, and Steven M. Bellovin “Privacy Enhanced Access Control for Outsourced Data Sharing” Financial Cryptography and Data Security Lecture Notes in Computer Science Volume 7397, 2012, pp 223-238.

[12] A. Fiat and M. Naor, “Broadcast encryption,” in Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, ser.CRYPTO ’93. London, UK:Springer-Verlag, 1994, pp. 480–491.

[13] Qianhong Wu, Yi Mu, Willy Susilo, Bo Qin, and Joseph Domingo-Ferrer. Asymmetric group key agreement. In Antoine Joux, editor, Euro crypt, volume 5479 of LNCS, pages 153-170. Springer, 2009.

AUTHOR DETAILS

MUTHUKUMAR. S Bachelor of Technology Degree in Information Technology from Kalasalingam University, Virudhunagar, India in 2012. Currently, pursuing Master of Engineering degree in Software Engineering from SNS College of Technology, Anna University, and Chennai. His area of interest are cloud computing, software development.

VIMALARANI. C received Bachelor of Engineering degree in Computer Science and Engineering from Anna University, Chennai, India in 2005, she pursued her Master of Engineering degree in Computer Science and Engineering. She is at present working as Assistant Professor (Senior Grade) in the department of Computer Science Engineering at SNS College of Technology, Coimbatore, India. Her area of interest includes Image Processing, Mobile Ad-hoc Network