Efficient Privacy Protection for e-Health Records over Mobile Cloudlet based on Advanced Security Mechanism

Tatimatla Sri Sai Rishitha, G. Krishna Mohan, J. Satish Babu

Abstract*: *Outsourcing medical data in e-healthcare systems with respect to data storage and sharing to different users is an aggressive concept in real time cloud computing applications. Privacy based medical data sharing is a challenging issues for secure data storage in cloud. However different types of security related approaches were achieved to access personal health information related services are explored into real time data sharing aspects in distributed environment. In privacy management of e-health data, scalability, cryptography, fine grained access control between different users is a basic issue to share patient's personal data in cloud. So that, in this paper, Novel Distributed Patient Centric Framework (NDPCF), which describes efficient mechanism for access control to different users in semi-trusted e-health care systems. To configure efficient scalable access control for patient's health care records we privilege the attribute based encryption (ABE) to encrypt and decrypt patient's health records. Our proposed approach also has dynamic modification access policies for different attributes user revocation at emergency situations. Extensive experimental results of proposed approach gives better and efficient security related results.

Index Terms*: *Cloud computing, personal health information, medical data assistance and access control.

I. INTRODUCTION

With the implementation of patient healthcare big data in vulnerable technology. Cloud assisted healthcare system becomes critical issue based on health consultation. Present day's e-health care system is an challenging task to personalize specific healthcare data for different users in fusion consultation for distributed environment. Through sharing of patient's data on social health data is beneficial to patients, sensitive data may be leaked by some of the authorized present in e-healthcare cloud systems. Procedure for data outsourcing in distributed environment shown in figure 1.

Medical storage e-healthcare systems, for example, user can acquire data from different data storage systems based on client's data. Different business related organizations can access data from e-health cloud storage systems. Each record in patients have their personal data like credit card and other information relates to e-health system.

So that, in this paper, Novel Distributed Patient Centric Framework (NDPCF), which describes efficient mechanism for access control to different users in semi-trusted e-health care systems. To configure efficient scalable access control for patient's health care records we privilege the attribute based encryption (ABE) to encrypt and decrypt patient's health records. Our proposed approach also has dynamic modification access policies for different attributes user revocation at emergency situations.

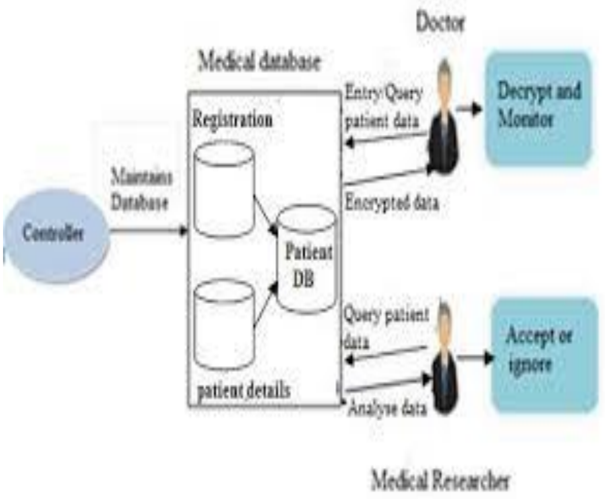


Fig. 1 Advanced privacy protection for patients in cloud.

Major contributions relate to proposed approach is as follows:

1. We propose novel ABE based approach for secure data sharing of personal healthcare documents and manage key management for different users with multi-user settings in outsourced cloud data.
2. Using attribute authority improves security in multi-authority attribute based encryption to avoid key-escrow problem in data sharing between different users in distributed environment.

II. PRIVACY PROTECTION & INTRUSION PROCEDURE IN CLOUD

Procedure relates to privacy protection cloud based healthcare systems procedure appear in figure 2.

The customer's physiological information are first gathered by wearable gadgets, for example, brilliant apparel [1]. At that point, those information are conveyed to cloudlet. The accompanying two imperative issues for social insurance information assurance is considered. The first issue is human services information security assurance and sharing information shown in figure 2(a), second component is reliable to keep medical services with outsourced data storage shown in figure

Revised Manuscript Received on May 07, 2019.

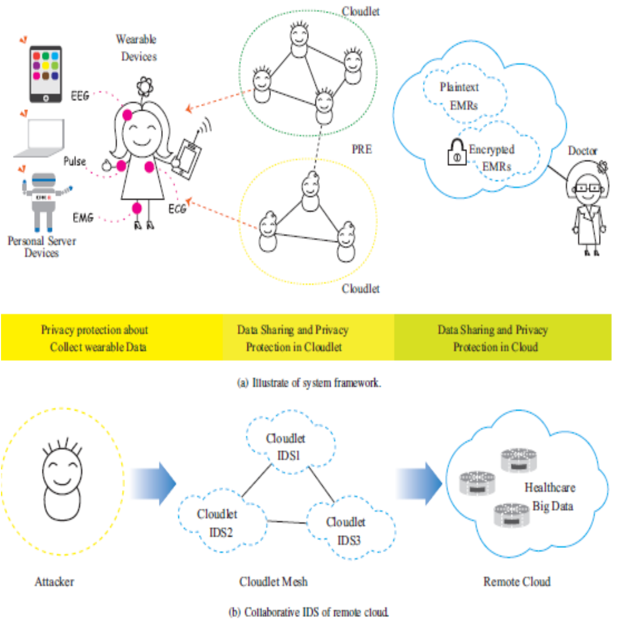
Tatimatla Sri Sai Rishitha, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India.

G. Krishna Mohan, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India.

J.SatishBabu, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, A.P., India.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

2(b). We address the main encryption and decryption procedure as follows.



(a) Illustrate of system framework.

(b) Collaborative IDS of remote cloud.

Fig. 2 Privacy protection and intrusion detection procedure with respect to different patients data.

Client information encryption. We use the model exhibited in [2], and exploit NTRU [3] to secure the customer's physiological information from being spilled or mishandled. This plan is to ensure the client's protection when transmitting the information from the cell phone to the cloudlet. • Cloudlet based information sharing. Ordinarily, clients topographically near one another associate with the equivalent cloud server. It is the basic scenario to share basic viewpoints, for instance, patients experience the ill effects of comparable sort of infection trade data of treatment and offer related information. For this reason, we utilize clients' closeness and notoriety as info information. After we acquire clients' trust levels, a specific edge is set for the examination. When coming to or surpassing the limit, it is viewed as that the trust between the clients is sufficient for information sharing. Something else, the information won't imparted to low confide in level.

Remote cloud server security concerns allow different services. Client share data in cloud, data described in remote server communication with restore data of patient’s data. For efficient secure storage of data in cloud, different approaches are described in [4][5] isolate with unique equivalent number of each patients. In group sharing of patient’s data then select appropriate privacy concern t remove irrelevant and duplicate data from cloudlet. If high amount of data present in remote server then basic security related approach is required. In this paper, we describe about communication buildup framework to explore and describe efficient data storage with privacy for efficient intrusion detection on cloud assistance.

A. Figures

As said, to insert images in *Word*, position the cursor at the insertion point and either use Insert | Picture | From File or copy the image to the Windows clipboard and then Edit | Paste Special | Picture (with “Float over text” unchecked).

The authors of the accepted manuscripts will be given a copyright form and the form should accompany your final submission.

III. PROPOSED APPROACH FRAMEWORK

In this section, we define the implementation procedure of proposed approach with respect to numerous clients. In this implementation, our proposed approach consists ABE framework. For each personal data sharing of patient every personal user identification is proved in proposed approach share personal details shown in figure 3.

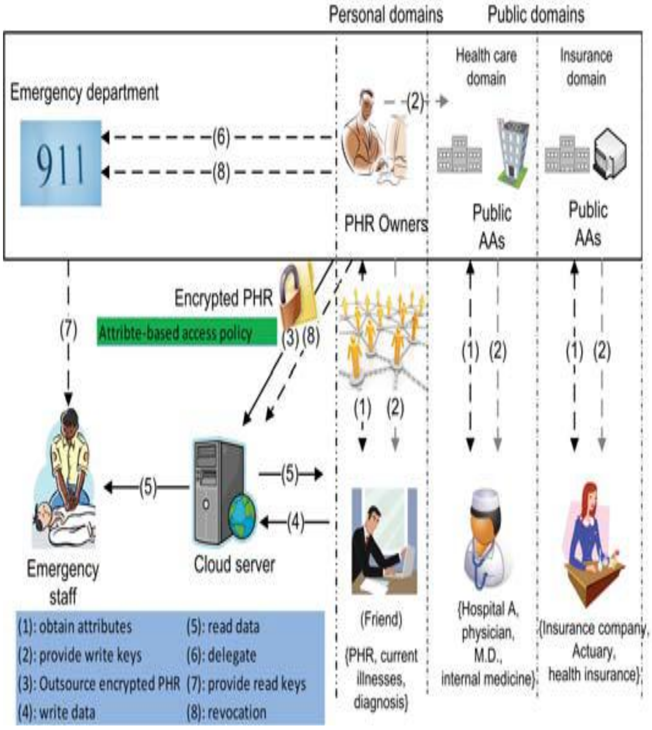


Fig. 3 Patient centric procedure to secure patients data in proposed framework System Implementation, Description

In this system, we describe universal attributes of each user based on personal health user identification using basic user profile related to medical healthcare systems. Emergency attribute selection is called as break glass access of user’s data. Each personal patient health care system each user generates master secret keys, the public master keys published in user’s storage in online social health care system. There are two basic distributing secret keys, first using healthcare system, owner can access privilege of personal health data based on the corresponding secret key, second, user can share secret key sending request to personal patient’s health data. Data owner grant permissions to access personal health data using the KeyGen and other operations in data outsourcing cloud data. Procedure of personal health data discussed in figure 4 with feasible conditions.

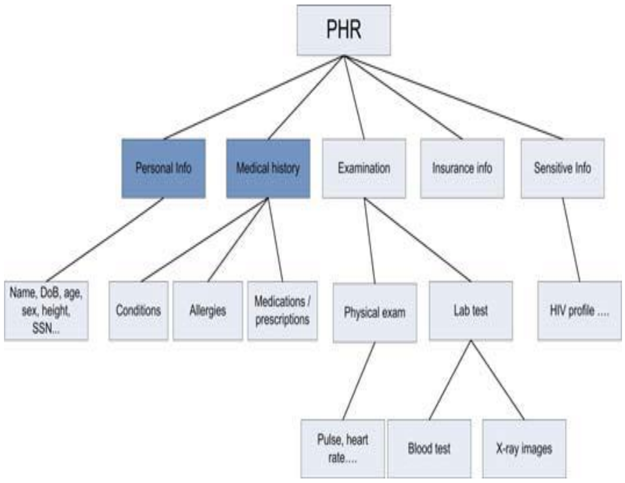
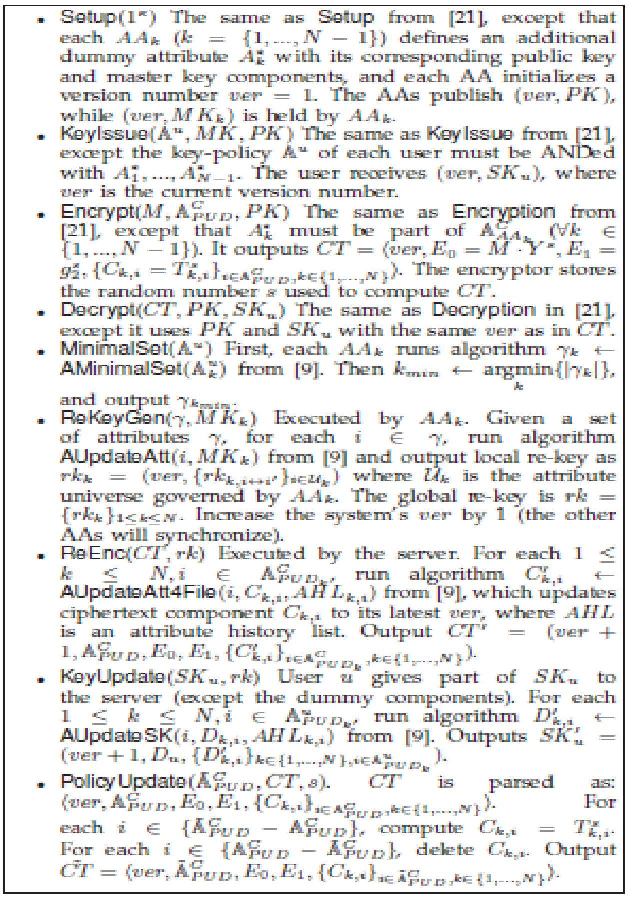


Fig. 4 Hierarchy of representation of different attributes with respect to stored patients data.

Furthermore, the information qualities can be composed in a various leveled way for productive strategy age, see Fig. 4. At the point when the client is allowed all the record types under a classification, her entrance benefit will be spoken to by that class.



- Setup(1^κ) The same as Setup from [21], except that each AA_k ($k = \{1, ..., N-1\}$) defines an additional dummy attribute A_k^* with its corresponding public key and master key components, and each AA initializes a version number $ver = 1$. The AAs publish (ver, PK), while (ver, MK_k) is held by AA_k.
- KeyIssue($\mathbb{A}^u, MK, PK$) The same as KeyIssue from [21], except the key-policy $\mathbb{A}^u$ of each user must be ANDed with $A_1^*, ..., A_{N-1}^*$. The user receives (ver, SK_u), where ver is the current version number.
- Encrypt($M, \mathbb{A}_{PUD}^C, PK$) The same as Encryption from [21], except that A_k^* must be part of $\mathbb{A}_{AA_k}^C$ ($\forall k \in \{1, ..., N-1\}$). It outputs $CT = (ver, E_0 = M \cdot Y^s, E_1 = g_2^s, \{C_{k,i} = T_{k,i}^s\}_{i \in \mathbb{A}_{PUD}^C, k \in \{1,...,N\}})$. The encryptor stores the random number s used to compute CT.
- Decrypt(CT, PK, SK_u) The same as Decryption in [21], except it uses PK and SK_u with the same ver as in CT.
- MinimalSet($\mathbb{A}^u$) First, each AA_k runs algorithm $\gamma_k \leftarrow$ AMinimalSet($\mathbb{A}_k^u$) from [9]. Then $k_{min} \leftarrow \underset{k}{\text{argmin}}\{|\gamma_k|\}$, and output $\gamma_{k_{min}}$.
- ReKeyGen(γ, MK_k) Executed by AA_k. Given a set of attributes γ, for each $i \in \gamma$, run algorithm AUpdateAtt(i, MK_k) from [9] and output local re-key as $rk_k = (ver, \{rk_{k,i \leftrightarrow i'}\}_{i \in \mathcal{U}_k})$ where $\mathcal{U}_k$ is the attribute universe governed by AA_k. The global re-key is $rk = \{rk_k\}_{1 \leq k \leq N}$. Increase the system's ver by 1 (the other AAs will synchronize).
- ReEnc(CT', rk) Executed by the server. For each $1 \leq k \leq N, i \in \mathbb{A}_{PUD_k}^C$, run algorithm $C'_{k,i} \leftarrow$ AUpdateAtt4File($i, C_{k,i}, AHL_{k,i}$) from [9], which updates ciphertext component $C_{k,i}$ to its latest ver, where AHL is an attribute history list. Output $CT' = (ver + 1, \mathbb{A}_{PUD}^C, E_0, E_1, \{C'_{k,i}\}_{i \in \mathbb{A}_{PUD_k}^C, k \in \{1,...,N\}})$.
- KeyUpdate(SK_u, rk) User u gives part of SK_u to the server (except the dummy components). For each $1 \leq k \leq N, i \in \mathbb{A}_{PUD_k}^u$, run algorithm $D'_{k,i} \leftarrow$ AUpdateSK($i, D_{k,i}, AHL_{k,i}$) from [9]. Outputs $SK'_u = (ver + 1, D_u, \{D'_{k,i}\}_{k \in \{1,...,N\}, i \in \mathbb{A}_{PUD_k}^u})$.
- PolicyUpdate($\tilde{\mathbb{A}}_{PUD}^C, CT, s$). CT is parsed as: $(ver, \mathbb{A}_{PUD}^C, E_0, E_1, \{C_{k,i}\}_{i \in \mathbb{A}_{PUD}^C, k \in \{1,...,N\}})$. For each $i \in \{\tilde{\mathbb{A}}_{PUD}^C - \mathbb{A}_{PUD}^C\}$, compute $C_{k,i} = T_{k,i}^s$. For each $i \in \{\mathbb{A}_{PUD}^C - \tilde{\mathbb{A}}_{PUD}^C\}$, delete $C_{k,i}$. Output $\tilde{CT} = (ver, \tilde{\mathbb{A}}_{PUD}^C, E_0, E_1, \{C_{k,i}\}_{i \in \tilde{\mathbb{A}}_{PUD}^C, k \in \{1,...,N\}})$.

Fig. 5 Step by step procedure for different data steps in data sharing.

For instance, in Fig. 4, a "sensitivity" document's traits are {PHR, restorative history, allergy}. The information per-users download personal health records PHR records from remote servers, and they can decode the records just on the off chance that they have appropriate secret keys ((5)). The information supporters will be allowed compose access to somebody's PHR, on the off chance that they present legitimate secret key((4)). Client Revocation. Here we think about denial of an information per-user or her properties/get to benefits. There are a few conceivable cases: 1) renouncement of at least one job characteristics of an open area client; 2) repudiation of an open space client which is proportional to disavowing the majority of that client's traits. Basic procedure used to protect keys with respect to patients stored data shown in figure 5 with different steps to process different scenarios.

As shown in figure 5, proposed approach describes different basic steps, first one is setup, key_gen generates different keys and then encrypt patient's data and then decrypt patient's data. Update each patients data based on secret-key with respect to access control policies in distributed environment.

IV. EXPERIMENTAL RESULTS

In this section, we describe the experimental setup of proposed approach in terms of generation of secret key, also describe communication and computation costs. We compare these results with conventional approaches in patient's health data sharing with respect to different privacy parameters. Based on these parameters we calculate the performance of proposed approach with existing approaches in terms of e-health data processing in cloud.

After performing above operations in uploaded file in e-health based cloud computing, the process to calculate time efficiency is given in Table 1 as follows:

Table. 1 Comparative analysis of key with respect to different users.

Key Depth	Average Time in secs
5	0.0524
10	0.05994
15	0.0745
20	0.0852
25	0.0954

Comparative evaluation for above mentioned table 1 as shown in figure 6.

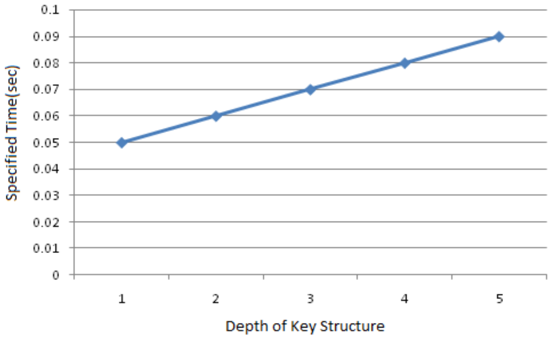


Fig. 6 Key structure with respect to different attributes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The scholar had performed data encryption and decryption of uploaded files in cloud computing based on attributes of uploaded file. The comparative analysis of proposed approach as follows:

Table. 2 Time efficiency comparison values for different attributes with different files.

S.No	Number of Attributes	Key Generation Time
1	10	0.9874
2	20	0.4012
3	30	0.5934
4	40	0.8124
5	50	0.9975

The process of encryption and decryption may perform in this approach is as based on attributes of the uploaded files with respect to time in number of files uploaded.

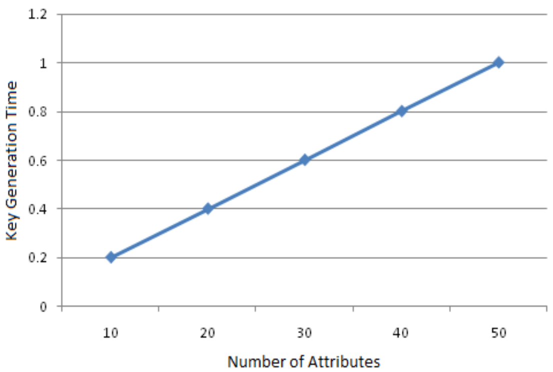


Fig. 7 Attributes for key generation for each patient health data in outsourced cloud.Based on results present in above discussion, we present the performance evaluation of proposed approach with respect to different attributes in key generation and other parameter sequences with different security notations.

V. CONCLUSION

In this paper, we propose a Novel Distributed Patient Centric Framework (NDPCF) for secure sharing of personal health records in cloud computing. Patient centric approach describes cloud server describes patients data confidentially and patients have complete privacy protection on their individual files through encrypt patients data with fine grained access control Our proposed framework address problem in data storage by multiple peoples store and share with owners and user's data then we successfully reduces the complexity in key management and enhance the privacy with comparison to existing approaches For efficient encryption, proposed approach use ABE to encrypt and decrypt patient's data and check allow permissions to users to modify or access patient's personal data in distributed environment. Experimental results of proposed approach gives better privacy related results in cloud computing.

REFERENCES

1. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.
2. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp. 417–426.
3. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.
4. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.
5. S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving hr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.
6. L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.
7. X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.
8. K. T. Pickard and M. Swan, "Big desire to share big health data: A shift in consumer attitudes toward personal health information," in 2014 AAAI Spring Symposium Series, 2014.
9. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.
10. J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin, "Self-protecting electronic medical records using attribute-based encryption," Cryptology ePrint Archive, Report 2010/565, 2010, http://eprint.iacr.org/.
11. M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp. 121–130.
12. X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.
13. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011.
14. S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-based access control in social networks with efficient revocation," in ASIACCS, Hong Kong, March 2011.
15. S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

AUTHORS PROFILE

Tatimatla Sri Sai Rishitha, pursuing M.Tech in the Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, completed BTech(CSE) from RVRJC College of Engineering, Her research interest mainly in Cloud Computing.

G. Krishna Mohan, working as a Professor of in the Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, and research interests are Software Engineering and Data Mining.

J.Satish Babu, working as Assistant Profesor in the Department of Computer Science and Engineering,KoneruLakshmaiah Education Foundation, Vaddeswaram, A.P.,India. His areas of interests are Data Mining, Software Engineering.