An Approach to Secure Data Sharing in the Cloud Using Proxy Re-Encryption for Data Security

K Chandra Sekhar[1], Mrs. M. Revati[2]

#1PG Scholar, Dept Of CSE, Nova College Of Engineering and Technology, Jangareddygudem.

#2 Associate Professor, Dept Of CSE, Nova College Of Engineering and Technology, Jangareddygudem.

ABSTRACT: As the Internet of Things has grown, data sharing has become one of the most beneficial cloud computing applications. Even though this technology has a pleasing aesthetic, data security is still one of its difficulties because inappropriate data utilisation might have a number of unfavourable impacts. In this paper, we present a proxy re-encryption technique for secure data transfer in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, and authorised users can access the data using proxy re-encryption construction. Because Internet of Things devices have limited resources, an edge device acts as a proxy server to handle computationally intensive tasks. Additionally, by utilising information-centric networking capabilities, we successfully distribute cached content in the proxy, thereby enhancing the quality of service and effectively utilising the network capacity. It accomplishes fine-grained data access control and lessens centralised system bottlenecks. Our strategy's potential to ensure data security, confidentiality, and integrity is shown by the security study and plan evaluation.

1.INTRODUCTION

The Internet of goods(IoT) has surfaced as a technology that has great significance to the world presently and its operation has given rise to an expanded growth in network business volumes over the times. It's anticipated that a lot of bias will get connected in the times ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes in operations analogous as healthcare, vehicular networks, smart cosmopolises, industriousness, and manufacturing, among others(1). The sensors measure a host of parameters that are truly useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and insulation. IoT needs to be secured against attacks that hinder it from furnishing

the demanded services, in addition to those that pose risks to the confidentiality, integrity, and insulation of data. A doable result is to reckon the data before outsourcing to the pall waitpersons. attackers can only see the data in its restated form when traditional security measures fail. In data sharing, any information must be restated from the source and only decrypted by authorized stoners in order to save its protection. Conventional encryption ways can be used, where the decryption key is shared among all the data stoners designated by the data owner. The use of symmetric encryption implies that the same key is shared between the data owner and stoners, or at least the actors agree on a key. This result is truly hamstrung. likewise, the data owners do not know in advance who the intended data stoners are, and, therefore, the restated data needs to be decrypted and subsequently restated with a pivotal known to both the data owner and the stoners. This decrypt- and- cipher result means the data owner has to be online all the time, which is nearly not realizable. The problem becomes increasingly complex when there are multiple pieces of data and different data owners and stoners Although simple, the traditional encryption schemes involve complex pivotal operation protocols and, hence, are not apt for data sharing. Proxyre-encryption(PRE), a notion first proposed by Blaze etal.(2), allows a deputy to transform a train reckoned under a delegator's public key into an encryption intended for a designee. Let the data owner be the delegator and the data user be the delegate. In such a scheme, the data owner can shoot restated dispatches to the user temporarily without revealing his secret key. The data owner or a trusted third party generates there- encryption key. A deputy runs there-encryption algorithm with the key and revamps the ciphertext before transferring the new ciphertext to the user. An natural particularity of a PRE scheme is that the deputy is not fully trusted(it has no idea of the data owner's secret key). This is seen as a high candidate for delegating access to restated data in a secured manner, which is a vital element in any data- sharing script.

2.LITERATURE SURVEY

2.1) FEACS: A Flexible and Efficient Access Control Scheme for Cloud Computing

AUTHORS: Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhount.

In the past few years, cloud computing has emerged as one of the most influential paradigms in the IT industry. As promising as it is, this paradigm brings forth many new challenges for data security because users have to outsource sensitive data on untrusted cloud servers for sharing. In this paper, to guarantee the

confidentiality and security of data sharing in cloud environment, we propose a Flexible and Efficient Access Control Scheme (FEACS) based on Attribute-Based Encryption, which is suitable for fine-grained access control. Compared with existing state-of-the-art schemes, FEACS is more practical by following functions. First of all, considering the factor that the user membership may change frequently in cloud environment, FEACS has the capability of coping with dynamic membership efficiently. Secondly, full logic expression is supported to make the access policy described accurately and efficiently. Besides, we prove in the standard model that FEACS is secure based on the Decisional Bilinear Diffie-Hellman assumption. To evaluate the practicality of FEACS, we provide a detailed theoretical performance analysis and a simulation comparison with existing schemes. Both the theoretical analysis and the experimental results prove that our scheme is efficient and effective for cloud environment.

3.PROPOSED SYSTEM

In our article, the data owner propagates an access control list which is stored on the blockchain. Only the authorized users are able to access the data. The contributions of this article are summarized as follows.

1) We propose a secure access control framework to realize data confidentiality, and fine-grained access to data are achieved. This will also guarantee data owners' complete control over their data.

2) We give a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.

3) To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IoT devices and as such provide high performance networking.

3.1 IMPLEMENTATION

Data owner:

Data owner will have to register initially to get access to the profile. Data Owner will upload the file to the cloud server in the encrypted format.

Cloud Server:

Cloud server will have Login then server can monitor file details and no owners and user details. And we have one sub module in cloud server I.e proxy. Proxy will reencrypted which is uploaded by data owner. then cloud server will give permissions for the users to access files .

User

In this module, there are n numbers of users are present. User should register before doing some operations . After registration successful he can login by using valid user name and password and location. After Login successful he will do some operations can access data from cloud.

Uses Of Our Approach

Data-centric solution with data protection for the Cloud Service Provider to be unable to access it.

Rule-based approach for authorization where rules are under control of the data owner.

High expressiveness for authorization rules applying the RBAC scheme with role hierarchy and resource hierarchy (Hierarchical RBAC or hRBAC).

Access control computation delegated to the CSP, but being unable to grant access to unauthorized parties.

Secure key distribution mechanism and PKI compatibility for using standard X.509 certificates and keys.

Multi-use. A multi-use scheme enables the proxy to perform multiple re-encryption operations on a single cipher text.

To Provide More Security.

IT makes use of cryptography to protect data when moved to the Cloud. Advanced cryptographic techniques are used to protect the authorization model in order to avoid the CSP being able to disclose data without data owner consent. Concretely, the solution is based on Re-Encryption (RE).

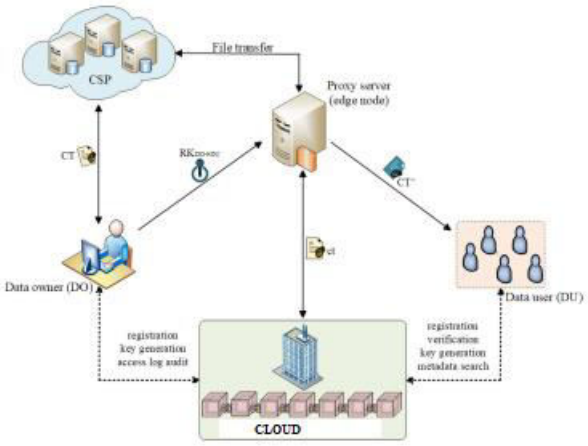

Fig 1:Architecture

4.RESULTS AND DISCUSSION

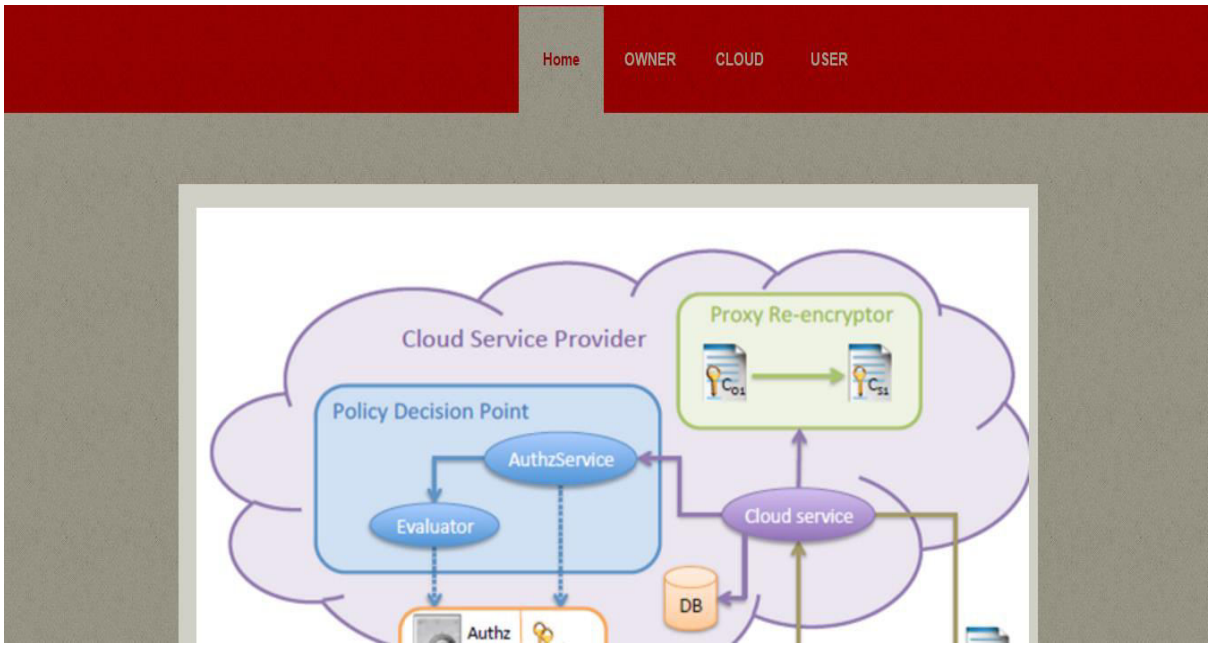

Fig 1:Home Page

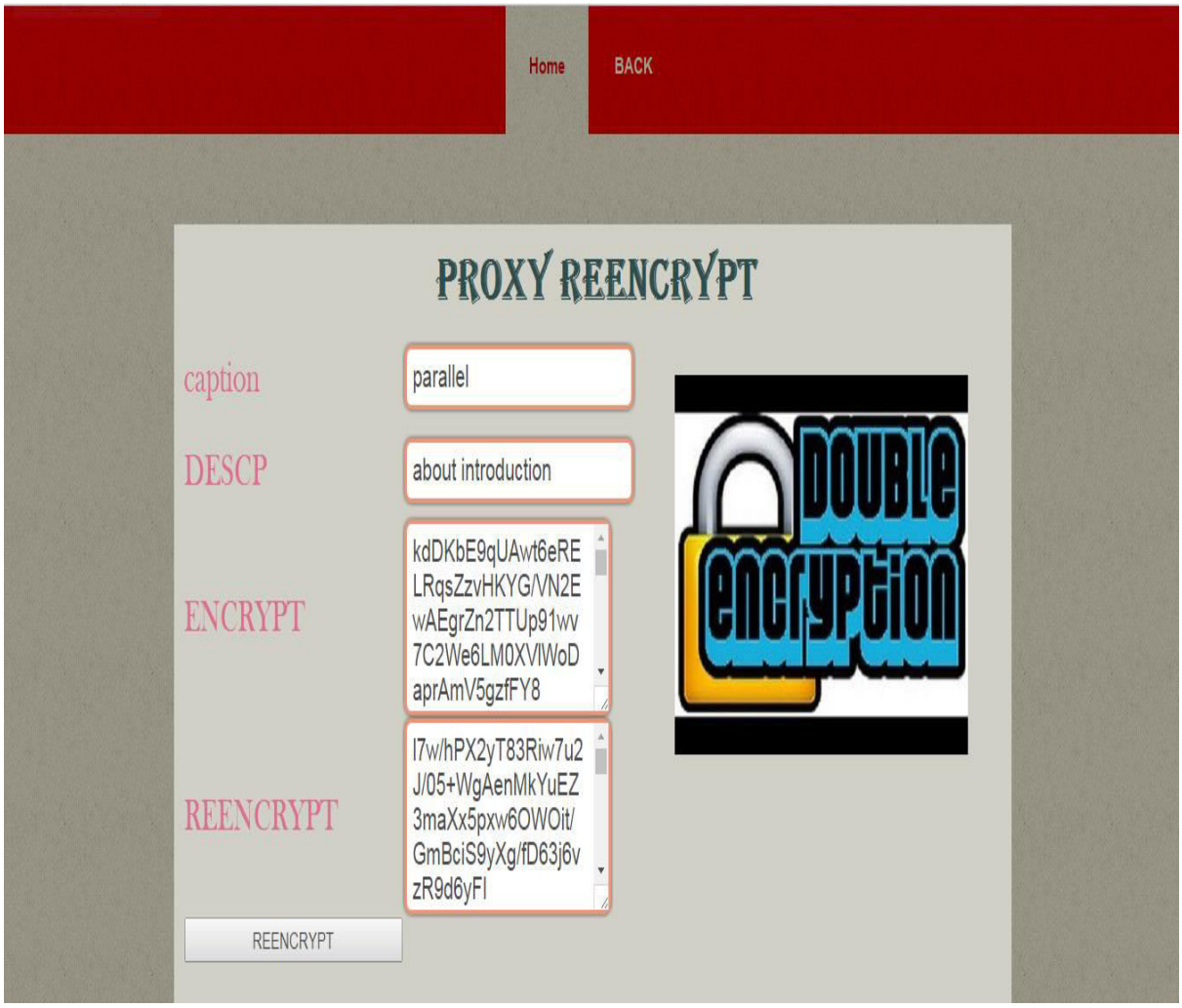

Fig 2:In the above screen we can see re-encrypted data

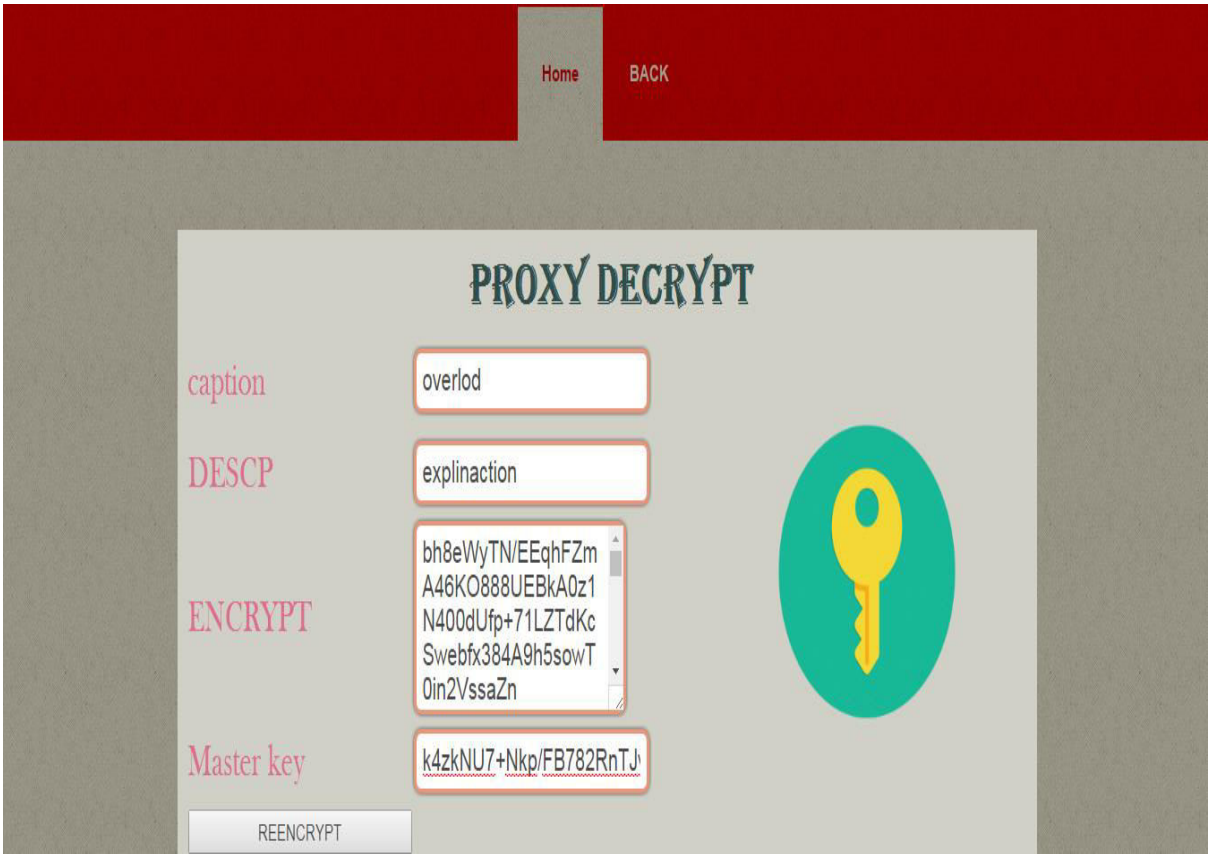

Fig 4:in the above screen use downloading information which was uploading by data owner by using master key

Fig 4:in the above screen use downloading information which was uploading by data owner by using Private key

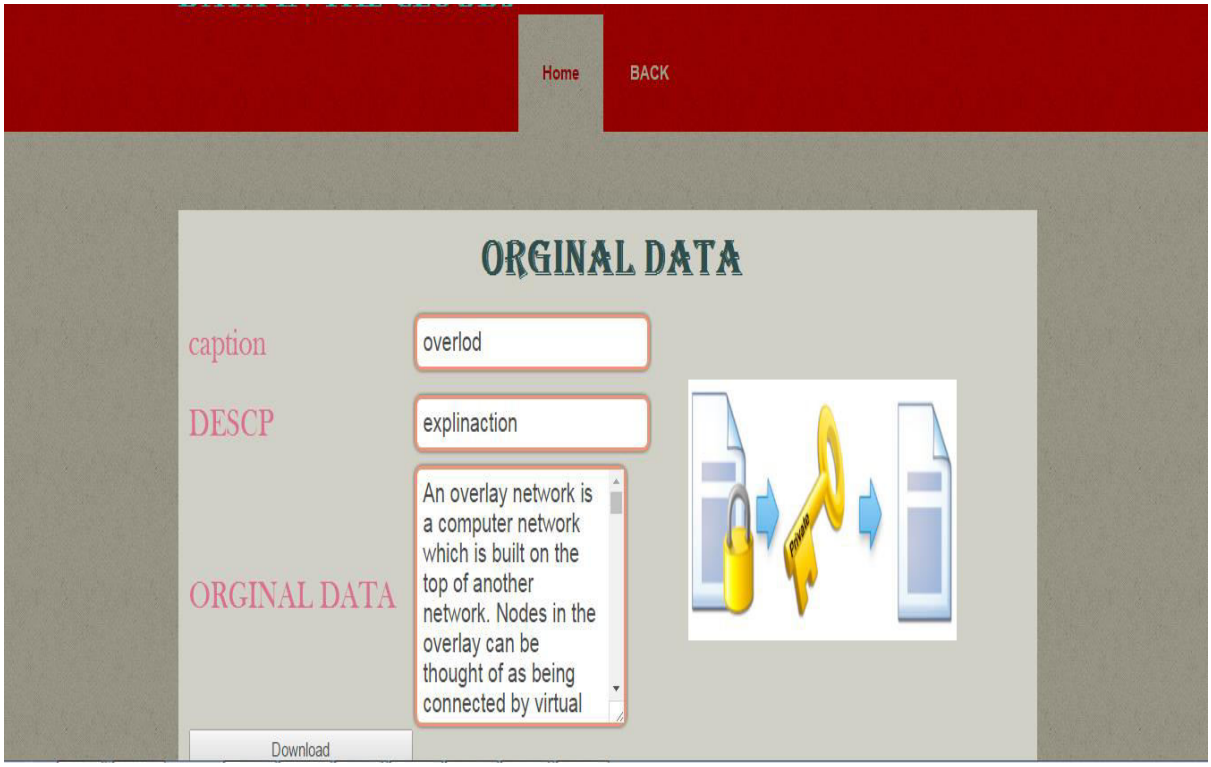

Fig 5:In the above screen we can see decrypted data by providing valid keys

5.CONCLUSION

Data sharing has come one of the IoT's most well- known uses as a result of its development. In a pall computing terrain, we give a secure identity- grounded PRE data- sharing medium to insure data confidentiality, integrity, and sequestration. The IBPRE technology enables secure data sharing and enables data possessors to effectively partake their translated data with authorised druggies while storing it in the pall. An edge device acts as a deputy to manage the violent computations due to resource limitations. The plan also makes use of ICN's capabilities to effectively serve cached material, enhancing service quality and optimising network bandwidth. also, we describe a system paradigm erected on a blockchain that enables flexible authorization for translated data. It's possible to apply fine- granulated access control, which can effectively help data possessors in conserving sequestration. The analysis and issues of the suggested model demonstrate how effective our plan is when compared to other plans.

[1] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v3.0,” CSA, Tech. Rep., 2003.

[2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, “Feacs: A flexible and efficient access control scheme for cloud computing,”in Trust, Security and Privacy in Computing and Communications, 2014 IEEE 13th International Conference on, Sept 2014, pp. 310–319.

[3] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.

[4] B. B and V. P, “Extensive survey on usage of attribute based encryption in cloud,” Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS ’06, New York, NY, USA, 2006, pp. 89–98.

[6] InterNational Committee for Information Technology Standards, “INCITS 494-2012 - information technology - role based access control – policy enhanced,” INCITS, Standard, Jul. 2012.

[7] E. Coyne and T. R. Weil, “Abac and rbac: Scalable, flexible, and auditable access management,” IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[8] Empower ID, “Best practices in enterprise authorization: The RBAC/ABAC

hybrid approach," Empower ID, White paper, 2013.

[9] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to rolebased access control," Computer, vol. 43, no. 6, pp. 79–81, 2010.

[10] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-encryption schemes with applications to secure distributed storage," ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1–30, 2006.

[11] F. Wang, Z. Liu, and C. Wang, "Full secure identity-based encryption scheme with short public key size over lattices in the standard model," Intl. Journal of Computer Mathematics, pp. 1–10, 2015.

[12] M. Green and G. Ateniese, "Identity-based proxy re-encryption,"in Proceedings of the 5th International Conference on Applied Cryptography and Network Security, ser. ACNS '07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 288–306.

[13] A. Lawall, D. Reichelt, and T. Schaller, "Resource management and authorization for cloud services," in Proceedings of the 7th International Conference on Subject-Oriented Business Process Management,ser. S-BPM ONE '15, New York, NY, USA, 2015, pp. 18:1–18:8.

[14] D. Y. Chang, M. Benantar, J. Y.-c. Chang, and V. Venkataramappa, "Authentication and authorization methods for cloud computing platform security," Jan. 1 2015, uS Patent 20,150,007,274.

[15] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets:A practically motivated enhancement to attribute-based encryption," in Computer Security - ESORICS 2009. Springer Berlin Heidelberg, 2009, vol. 5789, pp. 587–604.

[16] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS '10, New York, NY, USA, 2010, pp. 735–737.

AUTHOR'S PROFILE

K Chandra Sekhar pursuing M.Tech in department of Computer Science and Engineering at Nova College Of Engineering and Technology, Jangareddygudem.

Mrs. M. Revati, well known Author and excellent teacher Received M.Tech (SE) from Jawaharlal Nehru Technological University Hyderabad ,she is working as Associate Professor ,Department of computer science engineering , Nova college of Engineering and Technology, She has 11 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals. Her area of Interest includes Data Warehouse and Data Mining, information security, computer organization, flavors of Unix Operating systems and other advances in computer science.