International Journal of Science Engineering and Advance Technology

Efficient revocation and Data Retrieval in Cloud Storage using CP-ABE

Ch Amrutha[1], S V krishna reddy[2]
#1 M.Tech Scholar (CSE) and Department of Computer Science Engineering,
#2 Assoc.Prof, Department of Computer Science and Engineering, Kakinada Institute of Engineering and Technology for Women, Korangi, AP, India.

Abstract

As cloud computing ends up common, more encrypted data are being incorporated into the cloud. For the insurance of data protection, encrypted data more often than not need to be scrambled before redistributing, which makes powerful data usage an extremely difficult assignment. In this paper, we propose another technique to empower successful fuzzy keyword seek in a multi-client framework over encoded cloud data while keeping up catchphrase security. In this new framework, differential looking benefits are bolstered, which is accomplished with the strategy of characteristic based encryption. Data proprietors are inspired to store their profitable data in the cloud, now the issue emerges how to ensure significant data against assaults and dangers. In this paper we are presenting secure Attribute Based Encryption for ensuring profitable data and further quicker looking and getting to of encoded data dependent on programmed comment based seeking method.

Keywords: Data get to control, examining, CP-ABE, Cloud storage.

I. Introduction

Cloud computing is one of the developing field which replaces the weight of IT industry from spending enormous use on assets, for example, storage and system. Remote storage and simple availability of data joined with qualities, for example, on-request self-service, wide system get to, asset pooling, quick versatility and estimated services. Cloud is conveyed as open, private, cross breed and network cloud with service conveyance models, for example, SaaS (Software-as-a-Service), Platform-as-aService (PaaS) and Infrastructure-as-a-Service (IaaS). Assets in cloud are offered to the two ventures and people. However, cloud has numerous preferences certain issues, for example, security, protection and interoperability do exist. The main thrust for cloud computing is virtualization which empower different virtual machines to keep running with the assistance of single physical machine. As the foundation is being shared by a few VMs, security issues do emerge. Different overviews led depict security as one of the real test in cloud condition. Most recent provide details regarding cloud computing difficulties analyzes the issues and depicts that security remains as the principal challenge. Data confidentiality and protection issues do emerge due to multi-tenure normal for cloud. To shield customers from such issues, cloud service supplier need to pursue certain systems to guard data. Be that as it may, pernicious insider may follow up for the benefit of the supplier and send indelicate data. Such a circumstance makes a reasonable point that the security models can't be fabricate dependent on the trust of supplier. Customer needs to shield their data from pernicious assaults both remotely and furthermore from inward foes. Customers redistribute their files containing touchy data to cloud for compelling recovery at the essential time. Google look permits seek over plaintext data. Such data is being put away in plaintext shape in the cloud service which is powerless against assaults by foes. Insurance of data from such pernicious exercises is anticipated by putting away encoded data on cloud. Encryption strategies are delegated symmetric (AES) [1, 2] and awry (HECC) encryption calculations [7, 3]. HECC is turned out to be the strong strategy for scrambling and decoding files because of the hardness of hyperelliptic discrete logarithm issue. Consolidating such a calculation in cloud upgrades the data security in cloud condition. Data proprietors share their files with confirmed clients through recovery systems. Conventional techniques recover the whole accumulation of files for a solitary inquiry ask for from data client. This causes more opportunity for hunt answer and wastage of transmission capacity. Specific recovery of record

dependent on data client ask for makes utilization of catchphrases. Hunt of plaintext data isn't suited for cloud condition and encryption of data restrains the pursuit ability. Accessible encryption permits constructing a record with watchwords and relating reports. Trapdoors along ordering empower data clients to seek over encoded data in a protected way and keeps up security of archive data and in addition catchphrases. Such strategies stay inadmissible for cloud situations because of work of symmetric encryption techniques alongside single watchword look. With these traps it is fundamental for a compelling instrument to download scrambled records from cloud. The proposed model (Figure 1) fuses hilter kilter encryption, for example, HECC and position-based numerous catchphrase look plan to keep up data security and protection in cloud.

II. Related work

Nyamsuren Vaanchig et al (2018)this paper shows a Key-EscrowFree Multi-Authority Ciphertext-Policy Attribute-Based Encryption Scheme with Dual-Revocation by displaying "the essential property" and making use of a presentation specialist isolated from trait specialists. Differentiated and the present MA-CP-ABE designs, the proposed plot is the most sensible one to enable data get the opportunity to control for agreeable cloud storage structures. Besides, the security and execution examination demonstrates that our arrangement is more secure and sensibly powerful to be associated with rational circumstances as synergistic cloud storage structures. Mahesh Muthulakshmi, R et al (2018)Data access control is the trying issues out in the open cloud storage systems. In our paper the data security is upgraded using different authorities. Figure Policy Attribute-Based Encryption (CP-ABE) has been held onto as a promising techinque to give incessant, versatile, fine-grained and secure data get the chance to control for cloud storage with reasonable yet curious cloud servers. Mehdi Sookhaka et al (2017) This paper gives a thorough survey on attributebased get the chance to control designs and takes a gander at each arrangement's value and trademark. We also demonstrate a topical logical grouping of characteristic put together procedures based with respect to tremendous parameters, for instance, get the opportunity to control mode, building, refusal mode, denial methodology, disavowal issue, and renouncement controller. The paper reviews the forefront ABE procedures and masterminds them into three central classes, for instance, consolidated, decentralized, and hierarchal, in view of their plans. Krishnaselvi. L et al (2015)Cloud preparing is the movement of figuring services over the Internet. Cloud services empower individuals and associations to use programming and gear that are directed by pariahs at remote territories. We propose a subject that has distinctive key and third social gathering commentator for security. What's more, our affirmation and access control scheme is decentralized and incredible, unlike distinctive access control designs expected for clouds which are concentrated. Here simply real customers can disentangle the set away data. Ciphertext-Policy Attribute-Based Encryption (CPABE) Even anyway the definitions and advancements of different CPABE designs are not commonly exact, the businesses of the passageway structure in Encrypt and Decrypt computations are nearly the equivalent. Here we get the definition and improvement from [6, 10]. A CP-ABE plan contains four estimations: Setup, Encrypt, Key Generation (KeyGen), and Decrypt. Setup(λ,U) → (PK,MSK). The setup estimation takes the security parameter λ and the trait universe depiction Uas the data. It yields the general population parameters PK and an expert mystery key MSK. Encrypt(PK,M,A) → CT. The encryption computation takes general society parameters PK, a message M, and a passage structure An as data. The estimation will scramble M and convey a ciphertext CT with the true objective that elite a customer whose qualities satisfies the passageway structure will be fit todecrypt the message. We will expect that the ciphertext undeniably contains A. KeyGen(MSK, S) → SK. The key age figuring takes the pro mystery key MSK and a plan of traits S as data. It yields a mystery key SK. Decrypt(PK,CT, SK)→M. The unscrambling computation takes people in general parameters PK, a ciphertext CT which contains a passageway approach An, and a mystery key SK as information, where SK isa mystery key for a set S of characteristics. If the set S of qualities satisfies the passageway structure A, the figuring will unscramble the ciphertext and reestablish a message M. Incredible And Auditable Access Control (RAAC): In this paper, impelled by the heterogeneous designing with single CA and various RAs, we propose a generous and auditable access control plot (named RAAC) for open cloud storage to propel the

execution while keeping the versatility and fine granularity features of the current CPABE designs. In our arrangement, we seclude the system of customer legitimacy check from the mystery key age, and distribute these two subprocedures to two different kinds of specialists.

III. System Model and Security

Assumptions

We give the definitions of the system model, the security assumptions and requirements of our public cloud storage access control.

A. System Model

The system model of our design is shown in Fig. 1, which involves five entities: a central authority (CA), multiple attribute authorities (AAs), many data owners (Owners), many data consumers (Users), and a cloud service provider with multiple cloud servers(here, we mention it as cloud server.).

- The central authority (CA) is the administrator of the entire system. It is responsible for the system construction by setting up the system parameters and generating public key for each attribute of the universal attribute set. In the system initialization phase, it assigns each user a unique Uid and each attribute authority a unique Aid. For a key request from a user, CA is responsible for generating secret keys for the user on the basis of the received intermediate key associated with the user's legitimate attributes verified by an AA. As an administrator of the entire system, CA has the capacity to trace which AA has incorrectly or maliciously verified a user and has granted illegitimate attribute sets.

- The attribute authorities (AAs) are responsible for performing user legitimacy verification and generating intermediate keys for legitimacy verified users. Unlike most of the existing multi-authority schemes where each AA manages a disjoint attribute set respectively, our proposed scheme involves multiple authorities to share the responsibility of user legitimacy verification and each AA can perform this process for any user independently. When an AA is selected, it will verify the users' legitimate attributes by manual labor or authentication protocols, and generate an intermediate key associated with the attributes that it has legitimacyverified. Intermediate key is a new concept to assist CA to generate keys.

- The data owner (Owner) defines the access policy about who can get access to each file, and encrypts the file under the defined policy. First of all, each owner encrypts his/her data with a symmetric encryption algorithm. Then, the owner formulates access policy over an attribute set and encrypts the symmetric key under the policy according to public keys obtained from CA. After that, the owner sends the whole encrypted data and the encrypted symmetric key (denoted as ciphertext CT) to the cloud server to be stored in the cloud.

- The data consumer (User) is assigned a global user identity Uid by CA. The user possesses a set of attributes and is equipped with a secret key associated with his/her attribute set. The user can freely get any interested encrypted data from the cloud server. However, the user can decrypt the encrypted data if and only if his/her attribute set satisfies the access policy embedded in the encrypted data.

- The cloud server provides a public platform for owners to store and share their encrypted data. The cloud server doesn't conduct data access control for owners. The encrypted data stored in the cloud server can be downloaded freely by any user.

B. Security Assumptions and Requirements In our proposed scheme, the security assumptions of the five roles are given as follows. The cloud server is always online and managed by the cloud provider. Usually, the cloud server and its provider are assumed to be "honest-butcurious", which means that they will correctly execute the tasks assigned to them for profits, but they would try to find out as much secret information as possible based on data owners' inputs and uploaded files. CA is the administrator of the entire system, which is always online and can be assumed to be fully trusted. It will not collude with any entity to acquire data contents. AAs are responsible for conducting legitimacy verification of users and judging whether the users have the claimed attributes. We assume that AA can be compromised and cannot be fully trusted. Furthermore, since the

user legitimacy verification is conducted by manual labor, mis-operation caused by carelessness may also happen. Thus, we need an auditing mechanism to trace an AA's misbehavior. Although a user can freely get any encrypted data from the cloud server, Pages: he/she cannot decrypt it unless the user has attributes satisfying the access policy embedded inside the data. Therefore, some users may be dishonest and curious, and may collude with each other to gain unauthorized access or try to collude with (or even compromise) any AA to obtain the access permission beyond their privileges. Owners have access control over their uploaded data, which are protected by specific access policies they defined.

To guarantee secure access control in public cloud storage, we claim that an access control scheme needs to meet the following four basic security requirements:

- Data confidentiality. Data content must be kept confidential to unauthorized users as well as the curious cloud server.
- Collusion-resistance. Malicious users colluding with each other would not be able to combine their attributes to decrypt a ciphertext which each of them cannot decrypt alone.
- AA accountability. An auditing mechanism must be devised to ensure that an AA's misbehavior can be detected to prevent AAs' abusing their power without being detected.
- No ultra vires for any AA. An AA should not have unauthorized power to directly generate secret keys for users. This security requirement is newly introduced based on our proposed hierarchical framework.

IV. Data Access Control Models and Techniques

Data Access Control is one of the most important technologies to ensure adequate security of cloud computing. There was some traditional access control model which originated in the year of 1970s with the aim to prevent malicious users from accessing resources and avert them to use the potential resources illegally.

Access control mechanisms are a necessary and crucial design element to an application's security. In general, a web application should protect front-end and back-end data and system resources by implementing access control restrictions on what users can do, which resources they have access to, and what functions they are allowed to perform on the data. Ideally, an access control scheme should protect against the unauthorized viewing, modification, or copying of data. Additionally, access control mechanisms can also help to limit malicious code execution, or unauthorized actions through an attacker exploiting infrastructure dependencies (DNS server, ACE server, etc.).

Before selecting the data access control mechanisms, there are several fundamental steps that lend a hand speed up and elucidate the design process;

1. Try to quantify the relative value of information to be protected in terms of Confidentiality, Sensitivity, Classification, Privacy, and Integrity related to the organization as well as the individual users. Designing complicated and inconvenient data access controls around uncategorized or non-sensitive data can be counterproductive to the eventual goal or principle of the web application.

2. Determine the relative interaction that data owners and creators have within the web application. Some applications may restrict any and all creations or ownership of data to anyone but not the administrative or built-in system users.

3. Specify the process for granting and revoking user access control rights on the system, whether it is a manual process, automatic upon registration or account creation, or through an administrative front-end tool.

4. Clearly, delineate the types of role driven functions of application support. Try to determine which specific user functions should be built into the web application (logging in, viewing their information, modifying their information, sending a help request, etc.) as well as administrative functions (changing passwords, viewing any users data, performing maintenance on the application, viewing transaction logs, etc.).

5. Try to align access control mechanisms as close as possible to the organization's security policy. Much of information from the policy can map very well over the carrying out of access control

(acceptable time period of certain data access, types of users allowed in seeing certain data or performing certain tasks, etc.). These types of mappings usually work in the most excellent way with Role Based Access Control.

There are a plethora of accepted data access control models in the information security territory. Cloud computing is dynamic in nature and it supports the following traditional Access Control Models, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC). Data Access Control actually refers to the control over access to the various system resources after a user's account testimonials and distinctiveness have been legitimated and access to the system approved. For example, a specific user, or group of users, might only be given access to certain files after logging into a system, while simultaneously being deprived of access to all other resources.

A. Discretionary Access Control

Discretionary Access Control (DAC) is used to limit access to information based on the distinctiveness of consumers and/or membership in certain clusters. Access decisions are typically based on the authorizations granted to a user based on the credentials that the owner presented at the time of authentication (username, password, hardware/software token, etc.). Typically in DAC models, the owner of information or any resource is able to change its permissions. The downside of this method is overseer not been able to administer these authorizations on files/information loaded on the web server.

B. Mandatory Access Control

Mandatory Access Control (MAC) is the strictest among all levels of control and is primarily used by the government. MAC takes a hierarchical approach in controlling access to the resources. In this environment, the system administrator has sole responsibility for defining access control to all resource objects such as data files. In this model, security labels are assigned to all resource objects. These security labels contain two kinds of information - a classification (top secret, confidential etc.) and a category (management level, department or project to which the object is available).

When a user requests to access a resource, the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's testament matches the MAC security tag properties, the access is permitted. It is important to note, does both the classification and categories match. A user with top-secret classification, for example, cannot access a resource if they are not only a member in one of the required categories of that object. MAC requires a careful planning to implement. Once it is put into operation, it enforces a high system administration overhead due to necessitate evenly updating of object and accounting labels to have a room for new data, new users and modifications in the categorization and classification of existing users.

C. Role Based Access Control

Another name of this is called as Non-discretionary Access Control and uses real-world approach in structuring access control. Access under RBAC is based on user's profession function within the organization to which the computer system fits in.

Essentially, RBAC assigns special permissions to particular cadres in an organization. For instance, an accountant in a business will be allocated to the Accountant role, achieving access to all the resources legalized for all accountants on the system. Similarly, the developer role can be assigned to software engineer. A user under RBAC may only be assigned a single role in an organization. The accountant illustrated above obtains the same authorizations as all other accountants, nothing more and nothing less.

D. Rule-Based Access Control:

Rules-Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator. In this model, access properties are stored in Access Control Lists (ACL) associated with each resource object. When a meticulous account or group endeavors to access a resource, the operating system verifies the rules contained in the ACL for that resource.

Rules-Based Access Control includes conditions such as allowing access to an account or a group to a network connection in certain hours of the day or days of the week. As all access permissions are

controlled solely by the system administrator, the user cannot change anything.

VI. Security Issues Associated With the Cloud

Cloud computing is a prominent and fast growing technology has captured several professional attentions that allow many to store their data securely and the same can be accessed efficiently. Cloud service provider provides a variety of different service models such as Software-as-a Service, Platform-as-a-Service, Infrastructure-as-a-Service and deployment models as Private, Public, Hybrid, and Community. Nowadays many professionals have started to use cloud environment as it provides the user a storage capability to store and process their data. However, the challenges like data security and access control system are the main concern of Cloud Service provider.

Security concerns associated with cloud computing environment fall into two broad categories: security issues faced by Cloud Service Providers (CSP) (organizations providing software, platform, or infrastructure-as-a-service via the cloud) and security issues encountered by their consumers (companies or organizations who host applications or store data on the cloud). However, the responsibility is shared. The Cloud Service Provider must ensure that their infrastructure is secure and that their clients' data and applications are protected with well-defined cryptographic mechanisms, while the user must acquire measures to reinforce their application and apply strong passwords and authentication course.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers may use Encryption techniques to protect data in the Cloud. The security guidance of Cloud Security Alliance (CSA) recommends data is protected at rest, in motion and in use [30]. Encrypting data avoids illegal accessing of data in Cloud, but it might entail new issues related to access control management [31]. The most three important data security features are data confidentiality, availability, and integrity which prevents data loss].

- Data Confidentiality is a property of data, usually resulting from legislative measures, which prevents it from unauthorized disclosure.
- Data integrity is the overall completeness, accuracy, and consistency of data. This can be specified by the absence of modification between two instances or between two updates of a data record, meaning data is unbroken and unaffected.
- Data availability is primarily used to create service level agreements (SLA) and similar service contracts, which define and guarantee the service provided by third-party IT service providers.

b) Reasons to Use Secure Cloud Storage and Access Control:

When it comes to storing data in the cloud, it is important to deploy cost-effective technologies and solutions that protect, preserve and manage data to ensure that it is secure, available and accessible when needed.

The cloud, of course, can be a valuable tool in helping IT achieve this objective, but it is important to understand how, where and when cloud services should be used and when they shouldn't. Cloud works best and most cost-effectively when it is part of an overall data management strategy. Because data lifecycles evolve as an organization's data mix changes, you don't want to be locked into using the cloud. Rather, you want to be able to leverage cloud services when appropriate.

Nowadays most of the organizations have started to use public clouds such as Google App Engine (GAE), Amazon Web Services (AWS), IBM Blue Cloud and Windows Azure for storing, managing, processing and accessing their valuable data. The Cloud computing environment proposes diverse services to the user; however, data access service combined with enhanced security mechanism from the cloud plays a vital role. As per the 2017 – State of Cloud Adoption and Security studies, it is observed the following important insights, (i) in another 15 months, 80% of all IT budgets will be committed to Cloud apps and solutions. (ii) There is a tremendous growth in Hybrid cloud adoption, increasing from 19% to 57%. (iii) Public cloud adoption percentage has been improved. (iv) Many organizations today completely trust public clouds to keep their data secure. Public cloud platforms started to invest more for the development and resources in security features and support. To provide better storing and accessing the

data in Cloud computing requires advanced data access control techniques and security solutions.

From the survey, the access control model must provide a well strongly controlled data access facility to users and resources with enhanced security mechanism. It must also provide additional capabilities like access control manages user's files and other resources. From the point of access control, (i) cloud computing environment should provide Controlled data access to the various service of the cloud, based on the appropriate access control policies and the level of service requested (or) purchased by the user. (ii) Facilitate proper data access control policy and updated user's information. (iii) Cloud computing supports multitenant environment hence accessing data from one to another requires controlled data access policy. (iv)To ensure better and secure data access service within the cloud environment, there must be a strong relationship between trust and reputation in the data access control models. (v) Providing controlled access to both standard user files and privileged organizational functions. Major stumbling block in cloud computing data access control is a different set of users with diverse sets of enhanced security mechanisms such as storing, managing, processing and accessing of physical resources.

The issues related to data access control in Cloud computing environment can be solved with properly implemented data access control techniques with state-of the-art security solution and today's implementers can avoid such a issues made by the predecessors.

VII. Proposed System

Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Cipher text-Policy Attribute-Based Encryption (CPABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine grained and secure access control for cloud storage systems. In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labelled with his/her own attributes. Only if the attributes associated with the user's secret key satisfy the access structure, can the user decrypt the corresponding cipher text to obtain the plaintext. So far, the CP-ABE based access control schemes for cloud storage have been developed into two complementary categories, namely, single-authority scenario, and multi authority scenario. Although existing CP-ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation. Since there is only one authority in charge of all attributes in single-authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set.

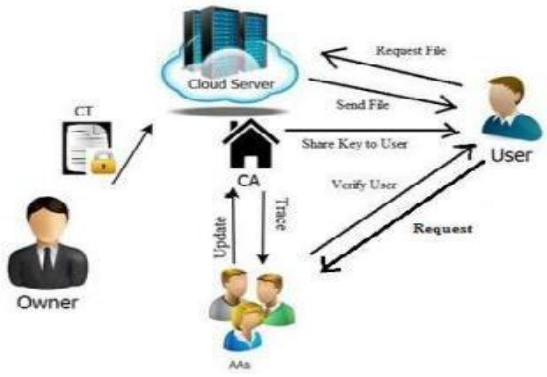

Fig. Proposed Architecture diagram

VIII. Conclusion

In this paper, we proposed a new framework to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CPABE cryptographic technique into our novel framework, our proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. Our scheme employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users' requests. We also proposed an auditing method to trace an attribute authority's potential misbehavior. We conducted detailed security and performance analysis to verify that our scheme is secure and efficient. The security analysis shows that our scheme could effectively resist to individual and colluded malicious

users, as well as the honest-but curious cloud servers. Besides, with the proposed auditing & tracing scheme, no AA could deny its misbehaved key distribution. Further performance analysis based on queuing theory showed the superiority of our scheme over the traditional CPABE based access control schemes for public cloud storage.

References

[1] Efficient Retrieval over Documents Encrypted by Attributes in Cloud Computing Na Wang, Junsong Fu, Bharat K. Bhargava, *Fellow, IEEE*, Jiwen Zeng IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. , NO. , 2017

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS,January 2010, LNCS. Springer, Heidelberg.

[3] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 2005.

[4] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS, 2006.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYPT, 2004.

[6] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. S. III, "Public key encryption that allows pir queries," in Proc. of CRYPTO, 2007.

[7]] L. Ibraimi, M. Asim, & M. Petkovic, Secure management of personal health records by applying attribute-based encryption, In Wearable Micro and Nano Technologies for Personalized Health (pHealth), IEEE,pp. 71-74, 2009.

[8] A. Bessani,M. Correia,B. Quaresma, F. André, & P. Sousa, DepSky: dependable and secure storage in a cloud-of-clouds, ACM Transactions on Storage (TOS), vol.9(4), pp. 12, 2013.

[9] A. Lewko, & B. Waters, New proof methods for attribute-based encryption: Achieving full security through selective techniques, In Advances in Cryptology–CRYPTO ,Springer Berlin Heidelberg, pp. 180-198, 2012.

[10] J.Bethencourt, A. Sahai, and B. Waters, Ciphertext-Policy Attribute-Based Encryption, Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

Authors

Ch Amrutha is pursuing M.Tech(CSE), in the department of CSE from Kakinada Institute of Engineering and Technology for Women, Korangi,.

Mr. S V KRISHNA REDDY is working as an Associate Professor in Department of C.S.E, Kakinada Institute of Engineering and Technology (KIET-W), korangi, Kakinada. He has 9 years of teaching experience. He has supported many students to publish many papers in both National & International Journals. His area of Interest includes DBMS, Data mining and data warehousing, mobile computing, uml&DP, Data structures, Design and analysis of algorithms.