CLOUD COMPUTING ENVIRONMENT USING SECURED ACCESS CONTROL TECHNIQUE

Mrs.B.Arulmozhi[1], Mrs.J.Pavithra[2], Ms.A.Sivasankari[3]

[1]Head of the Department (BCA), Dept of Computer Science and Application, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.
[2]Research Scholar, Dept of Computer Science and Application, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.
[3]Head of the Department (B.Sc), Dept of Computer Science and Application, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.

Abstract - *Cloud computing has considerably reduced the computational and storage costs of outsourced data. The existing access control techniques over user's access provisions centered on the frequent user attribute like role, which reduce the small-grained admission, calculate that provides the user an exclusive access through the use of a hierarchical formation which is a combination of user's single and widespread attribute. Also, we deploy the concept of voucher yielding system that allows the users to authenticate the correctness of outsourced data without the retrieval of the respective files. The tokens are derived from the Meta data containing file position that helps in the process storage correctness verification and improvises the storage efficiency. The untried results show SCFAP has superior storage efficiency and error recovery measures than existing techniques.*

Key Words: *Access control, access formation, barrier limits, storage efficiency, token granting system….*

1. INTRODUCTION

Cloud computing is one of the widely used emerging technique that offers various methods to acquire and manage IT resources on a large scale. Cloud computing in turn provides different types of services such as Infraformation as a service also sometimes called as hardware as a service, Platform as a service and Software as a service. Cloud computing planning promotes the resource sharing in a pure plug and provides a model that dramatically simplifies it's Infraformation. The advantage of cloud computing includes accessibility and cost effective in accessing the resources over the Internet. Employing the resources in the cloud provides greater expediency to the user because of its systematic manner. Cloud helps us to make use of the existing technologies such as virtualization, service orientation and grid computing in large-scale distributed environment. To assure the cloud data integrity and availability, efficient approaches that enable storage correctness assurance on behalf of cloud users have to be premeditated. Hence, cloud operations should also imperatively support the dynamic features that make the system design even more challenging.

This scheme ensures the property of scalability through the extension of ASBE (Attribute Set Based Encryption) technique. It defines a hierarchical formation that delegates the operation of trusted authority and private key generation to the domain authorities of the lower level. Here the user attributes were converted into the stable formation of the recursive type that permits the users to define constraints dynamically by representing a different combination of attributes, which satisfies the user access policy. As Cloud computing is a new emergent technology despite having many beneficial factors, it faces many threats in various ways.

It has spread very fast due to its flexibility over ease of access as it eliminates the need for extra hard drives and memory space allocation. As the cloud is a distributed system, the data stored in it is widespread in distinct locations and it is accessed anywhere. The distributed nature of the data creates the requirement for high security over outsourced data as there exists a probability that anyone can exploit the outsourced data. The hackers can also access the outsourced data by hacking any server virtually and the statistical results the system.

2. RELATED WORKS

2.1.1 Cloud based Access Control Techniques

It provides a multiauthority CBACT me with data decryption and user revocation functions. This work furthers a general Data Access Control Scheme that provides secured user data access even at weaker safety assumptions. The security analysis results of this scheme prove that this scheme is collusion resistance but lacks at the property of access provision to the individual users of the system.

The ID based cryptographic system makes use of the user quality such as user id for encryption and decryption process of the out sourced data. The expansion of ID based cryptographic scheme provide the secured data storage space over the public cloud and enhanced client agreement for other users to access the data content.

In work done by integration of cryptographic techniques with RBAC techniques was made and it uses role keys for data decryption. Further this work presents a hybrid cloud architecture, where the public cloud contains the basic level details and most sensitive information over the private cloud. This work separates the property of user delegation to active and passive types and establishes role management through the use of delegation servers and protocols. The Cipher text Policy Attribute Based Encryption was given by; it realizes the complex access control mechanisms over the encrypted data Here the attributes expressed solitarily the user credentials and the person who encrypts the data could access limit to the users for data decryption. Through the use of this scheme, the data stored could be kept condential even though it resides on the untrusted server.

2.1.2 Token Based Access Verification Systems

Proposed a flexible distributed storage integrity auditing mechanism that consists of homomorphic tokens and data. Tokens are provided to the users from randomly chosen block indices from each data vector space analogous to the memory location of the user requested file in the cloud. The use of erasure coded data technique protects the user data and eliminates the system errors such as data redundancy, fault tolerance and server crashes. In Privacy Preserving Public Auditing for Secure Cloud Storage by comprises a third party auditor (TPA) for auditing the integrity of outsourced data; this eradicates the new threats and realizes the data privacy. Experimental analysis of their proposed scheme proves that it provides high efficiency against Byzantine failure, unknown user attacks and attacks on cloud data modification. Access control schemes based on the token system were developed to provide greater security over the cloud storage systems. This scheme uses random masking technique integrated with a homomorphic authenticator that ensures the privacy of public auditing. Flexible distributed storage integrity checking mechanism is proposed by using homomorphic tokens and it avoids security problems like identifying unknown users. Through the use of homomorphic tokens and distributed erasure coded data, users were permitted to audit the outsourced data. This auditing allows the users to identify both the improper data access and cloud server misbehaviors. This scheme even ensures the cloud data security, which allows the users to perform dynamic operations efficiently over the outsourced data.

2.2 Comparison of Related Works

SCFAP scheme and HASBE scheme given by and the flexible integrity auditing mechanism.

2.2.1 Work by HASBE

To ensure the property of scalability and flexibility over outsourced data, a solution is presented in work. This work shows a Hierarchical Attribute Set Based Encryption (HASBE) scheme to cloud users, which extends the property of Cipher text attribute set based encryption technique. This scheme not only aims in the achievement of scalability, it even inherits the property of flexibility and small-grained access provision through the management of compound attributes.

The HASBE scheme makes use of multiple value access expiration time to deal with user revocation problems. The first part of this work describes the extension of HASBE from ASBE technique using the hierarchical formation. Whereas the second part provides a clear demonstration of the implementation of access control scheme based on HASBE for cloud computing.

The cloud service provider provides services to users. The data owners share their data contents through the cloud in an encrypted manner. Data consumers decrypt the shared contents to perform their respective access operations. Each data owner and data consumer was assigned with a domain authority, where each domain authorities could be managed through parent domain authorities or trusted domain authorities. The major responsibility of every domain authority is to administer the domain authorities at next level or the data owner or consumer in its domain.

In HASBE scheme the data users were only assumed to possess read access. All the entities associated with this scheme were organized in a hierarchical manner to accomplish their tasks. A recursive set based key formation is formed for every user, where each element of the set is either a set or an element corresponding to a user attribute. The depth of the key formation is found using the level of recursions in the recursive set, which is similar to the definition of depth tree. At mandatory that all the members of the set should be of attribute elements. A unique label for the user attributes was formed using key formation. The access formation to the users in HASBE was formed in a similar way to the ASBE scheme given by. In access tree formations the leaf nodes were considered to be the attributes, and represent the threshold gates. The nodes were defined using its children and threshold values.

This work provides user access provision with the help of the hierarchical access formation, and it is formed using appropriate user key formation and access formations. It means that the user with private key corresponding to attributes in key formation would be able to access the data, only when their attributes satisfies the access policies defined by the access formation.

System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access and File. Each major system operations related to the HASBE scheme invokes the appropriate algorithms associated with it to accomplish their tasks, and it works by bilinear mapping concepts.

Though system provides a better solution to scalability and flexibility issues, the complete support for compound values and multiple value assignments are measured and found to be lagging in efficiency. This reduces the level of small-grained data access. The proposed SCFAP scheme defines users with their role based classification. Provides efficient support for compound attributes and multiple value assignments.

The hierarchical formation described in SCFAP scheme improves the level of small-grained access provision associated with individual users of the system. The HASBE scheme future does not allow write access to the data users of the system. This makes its application inappropriate to critical systems like financial sectors, where several users require write operations to be performed. SCFAP scheme allows the users to perform write operations in an effective manner and it is achieved through the use of token granting system, which preserves the storage correctness of the outsourced data.

2.2.2 Work by SCSAP

Approaches to form solution for security risks accompanying the correctness of physical possession over outsourced data were done by. This work presents a flexible distributed storage integrity auditing mechanism, which ensures the correctness of outsourced data through the use of homomorphic token and distributed erasure coded data. This scheme provides efficient user auditing of cloud data with very lightweight communication and computation cost. The auditing result provides both storage correctness guarantee as well as fast data error localization (identification of server misbehaviors). It even allows user access operations over outsourced data including block deletion, modification and appends functionalities.

The overall contribution of this work is summarized as follows:

1) This scheme further supports secure and dynamic operation over data blocks including update, delete and append.

2) The work further makes an extensive security analysis that shows its resistance towards Byzantine failures and malicious data modification attack and server colluding attacks.

3) In comparison to many of its predecessors, this scheme achieves both the storage correctness insurance and data error localizations.

The flexible integrity auditing mechanism discussed in this section consists of four major entities, which includes User, Cloud Service Provider (CSP), Cloud Server (CS) and Third Party Auditor (TPA). Users share their data through cloud storage services, and a user can be either enterprise or an individual customer. Cloud Server (CS) is managed by the CSP to provide better computation and storage facilities to the users of the system.

TPA is an optional entity with expertise qualities that user does not possess. TPA assesses and describes the risk of cloud storage services on behalf of users upon request. This work provides more focus towards file oriented data rather than nonfile oriented applications like social net working systems.

Block level operations over user data were considered as block update, block delete, block insert and append operations. The major focus of this work is to identify the key integrity issues like unauthorized data modification and corruptions, caused due to server compromises and random Byzantine failures.

Users store their valid credential to cloud servers through CSPs. The problem of data redundancy could be employed through the technique of erasure correcting code. This scheme further tolerates faults and server crashes that happen due to increasing data users. The users interact with cloud servers for processing file retrieval request through CSPs it is necessary to verify the correctness and maintenance of the cloud data. The users were provided with the precomputed tokens that provide correctness assurance to the users of the system.

Tokens are derived from the subset of file blocks in a random manner. The verification token helps the users to ensure correctness of data operation request processed by the CSP. Tokens are issued to the user based on randomly chosen block indices from each data vector space corresponding to memory position of the requested file in the cloud and data. In cases of inappropriate situations like insufficient resources and time the users can delegate their responsibilities to TPA. This work achieves secure data storage through five major steps, which includes file distribution preparation, challenge token precomputation, correctness verification and error localization, file retrieving and auditing and finally, towards third party auditing.

This scheme provides an approach methodology that prevents CSP to process data dynamics without knowing user secret key materials and ensures users that dynamic data operation request done by CSP were processed faithfully. The algorithms associated with each stage helps in the management of activities accompanying data storage management and correctness verification processes.

Tokens were provided to the users, based upon randomly generated block indexes and memory position of the file. This makes the property of storage correctness associated with integrity auditing scheme to be a probabilistic feature. The proposed SCSAP scheme solves this issue by granting tokens to the users in a deterministic manner. In SCSAP scheme tokens were derived from Metadata

containing file locations and distributed to all the users of the system during appropriate phases.

3. CONSTRUCTION OF STORAGE CORRECTNESS AND SMALL-GRAINED ACCESS PROVISION TECHNIQUE

3.1 System Design

This section presents a conceptual design of the novel scheme called Storage Correctness and Small-grained Access Provision (SCSAP) scheme. The proposed SCSAP scheme consists of two parts. The first part deals with the construction of hierarchical based user access formations and the second part depicts the algorithmic phases associated with SCSAP scheme that helps in the achievement of small-grained data access and improved storage efficiency across the out sourced cloud data storage.

A set of appropriate cryptographic keys and access formations derived from the exact user attributes were distributed to all the users of the system. Through the use of the access formations and cryptographic keys every user of the system performs the cloud data access in a secure way.

As a result of the encryption process, both the data owners and users were provided with a token, which assists in the process of integrity and security verification over the outsourced data. The proposed system consists of five major entities and the descriptions to the entities were given as follows, Attribute Authority (AA): The major responsibility of the Attribute Authority (AA) is to manage all the attribute related activities in specialization with the activities confining to the management of user roles. This includes maintenance of role revocation, delegation, key allocation to users and authentication of the user given credentials like the public key, private key, etc.

Cloud server (CS) performs all the computation related activities. This includes the computation of user given inputs and producing corresponding computational results and acknowledgments to the users. Cloud Service Provider (CSP) provides services to the users of the system and performs the validation of the user given inputs and outputs during the process of encryption and decryption. Service Consumers (Users).

A Service consumer is also called as the user of the system, consumes the services provided by the cloud computing environment. Data Owner: Shares valid data contents over cloud computing environment and fixes data access limits across data users.

3.2 Assumptions

The hierarchical formation described in this paper is assumed to provide many-to-many data sharing in a secured manner through which the property of small-grained access control, confidentiality, and non-repudiation of the outsourced data was achieved.

3.3 Key Terminologies

3.3.1 Hierarchical Formation

The hierarchical formation defines the access policy associated with the individual users of the system. A hierarchy is framed from the combination of the user unique and common attributes. Each hierarchy represents the one to one relationship between the user and their access policies. The access policy defines the set of operations (read or write access) the user could perform over the outsourced data.

3.3.2 Key Formation

Key formations were designed to preserve the security of the outsourced data. Key formations are derivatives from the user common attributes like roles. The formation of key formation assigns the access privileges to the set of the common users over the outsourced data. This states that users beneath a particular role were assigned with a key formation such that they could gain access to a particular set of files.

3.3.3 Access Formation

Access formations were designed to achieve the property of small-grained user access and it is derived from the user unique attributes like user id. It defines the extent to which an individual user could access the data.

3.3.4 Grade

Grade denotes the level of the extent to which the set of common users could gain access to a particular set of files. Each grade formally represents a key formation, such that a user with certain grade could gain access to all the files that comes with the scope of a particular grade. Grades were derived from the user common attributes like dep id, such that it represents a set of files that belongs to the particular department.

3.3.5 Barriers

Barriers are restrictions imposed over the grades to achieve the small-grained user access level. To solve this issue, barriers were designed and imposed over the user grades.

3.3.6 Tokens

Tokens were derived from the metadata containing the file location and it acts as a user authentication entity. Tokens were issued to the data users as a result of the data

encryption process. Since the token represents the Metadata about the file location, it assists in the process of easier file retrieval. This improves the storage efficiency of the proposed system. A new method of mathematical modeling was used to identify the functions and variables of the proposed scheme.

4. PRELIMINARY CONCEPTS AND ALGORITHM

4.1 Secret key

Secret Key is a basic algorithm for symmetric algorithm through which all the other keys associated with the data users were derived. This algorithm is invoked automatically whenever the process of key generation is required. It could be of any other key like master key, public key and private key.

4.2 Formation of Hierarchical Access Formation

The proposed SCFAP scheme makes use of the hierarchical access formation to define the user access rights. The basic concept behind the hierarchical access formation was described in the previous section of the paper.

In an organization the most important or most secured files could be accessed only by the personals at the topmost designation order, least important files by the low level personals and ordinary files could be accessed by the midlevel individuals.

In SCSAP scheme each user is assigned with a hierarchical formation, which is derived from their respective key and access formations. Key formation is premeditated to preserve the security of the outsourced data and it represents the access rights to the group of users with a common identity. The basic concepts behind the formation of the key formation were given in the previous section.

4.2.1 Access Formation

The access formation represents the access rights to the individual user of the system. Even though a particular user is assigned with a grade representing the key formation, it is not mandatory that the user could access all the files that come under a particular grade. The access formations associated with the SCSAP scheme were designed in such a way that solves the problem of above mentioned issue. The Barriers are restrictions that were imposed over the user access grades to achieve the small-grained access control. The assignment of the access formation defines the individual access limits over the set of files. In addition to this, phase 3 of the storage correctness scheme provides a brief summary about the algorithmic implementation of the user access formation assignment.

4.2.2 Token Granting System

The proposed SCSAP scheme makes use of the token granting system through which the property of storage correctness is achieved. As it is described at the previous section tokens were derived from the Meta data containing the file location that assist in both ways, through which the process of storage correctness as well as the easier retrieval of the outsourced files could be made.

The prime idea behind the use of token granting system in SCSAP scheme is that at the end of every successful data encryption process the data users were provided with the tokens, through which the data users verifies the existence of the outsourced data. The users could also be able to perform the decryption process only when the Meta data of the user given token points to the user requested file.

5. ADVANTAGES OF PROPOSED SCSAP SCHEME

1) Through the use of the barrier limits in user hierarchical access formation helps in the achievement of small-grained access rights to the users of the system.

2) The algorithmic deployment of the token granting system helps in the achievement of the storage correctness verification of the outsourced data with improved storage efficiency.

3) The tokens were derived from the Meta data containing the file location. This reduces the file retrieval time associated with the user data access request.

6. EXPERIMENTAL STUDY

6.1 Deployment of SCSAP over Eucalyptus Cloud

The proposed SCSAP scheme runs at the Infraformation layer of the eucalyptus, and it works on a layered basis to accomplish its tasks. The SCFAP scheme consists of four layers such as user registration layer, authentication layer, access security management layer and instance management layer. The registration layer performs the user registration process. Authentication layer validates the cloudlet credentials, and the access security management layer allows or denies the user file access requests to the virtual machines with the aid of the functionalities present in the instance management layer.

An application is created in Eucalyptus an open source cloud platform, which deploys the proposed SCSAP scheme. An interface is developed using JSP to enable users to authenticate and view the cloud storage. Eucalyptus consists of several other interfaces like cloud42, AWST anacasino, EC2 Dream. MySQL community server5.7 is used for storage purposes.

The application consists of the Command Line User Interface (CUI) using Euca2ools, which allows the users to interact with the system. Every subject creates objects and requests their corresponding object access through the proposed SCSAP scheme that preserves the storage correctness and small-grained access provision of the user data. The security management layer controls and directs the access control schemes. The implementation consists of the web interface that possesses the property of ease of use through which the Cloud Service Providers (CSP) or Attribute Authorities (AA) creates the restriction over the cloud instances. The implemented SCSAP scheme allows the AA to manage access to cloud resources, instances, virtual machines and common user groups associated with the cloud computing environment.

The first step associated with the implementation of SCSAP scheme over eucalyptus cloud consists of the setup phase. Once the subject is registered with the system, the AA adds the subject to the common user groups. This states that all the subjects under the common user group contain the common access privileges with particular individual restrictions. These restrictions were imposed on the subjects through the assignment key formation and access formation to the subjects. Every subject can create new objects and gain access to existing objects based upon the following access restrictions:

1) Grades: Defines the level of the extent to which a common user group can access.

2) Barriers: Defines the level of extent through which an individual user can access.

3) Tokens: Derived from Meta data containing file location.

Each subject shares their newly created objects to the other subjects of common user groups. The subject can also share their objects to other Common User groups which they were not a member. To gain access to the shared objects and instances the subject accessing the object could not violate the SCSAP access policy.

Each subject could ensure the property of integrity over their respective subjects through the use of token granting systems. An updated token would be distributed to every subject associated with the shared object in case of modification to the shared data objects.

The implemented SCSAP consists of two distinct types of interfaces that include subject management and object management interfaces. The subject management interface assists in the management of all the subject related activities that include subject authentication, user common group assignments, subject key allocation, and management. The object management interface is responsible for the process of management of all the object related activities that include object storage, object retrieval, token generation, token computation, and management.

6.2 Validation of Premises

Built on the open source cloud platform Eucalyptus the application of SCSAP scheme to the developed prototype could be validated through the verification of which are described as follows:

1) Each subject should be assigned with an appropriate hierarchical access formation.

2) Encryption and decryption processes could be performed when the subject given inputs are valid.

3) Token computation results should match with the user given token and the user given file access request.

4) Each authenticated subject should be assigned to the common user group.

6.3 Access Verification Tests

The first test comprises the access request to the object from the subject who is not the member of the any of the common user group associated with the developed system. The request would be denied by the setup algorithm present at the authentication layer. The next test comprises the file access request from the subject with inappropriate hierarchical access formation.

The request for encryption or decryption processes with inappropriate cryptographic keys or inputs by the subjects is blocked through the several algorithms like Setup, GradeGen, BarrierGen, Token computation and Encrypt or Decrypt algorithm present at the user registration layer, Authentication Layer Security management layer and instance management layer of the developed prototype.

This request is blocked by GradeGen and AccessGen algorithms functioning at the access security management layer. A subjects access request for an object with invalid user credentials like invalid tokens and the secret key is denied, and the subject is blocked from accessing the services if he repeats the same for three times.

7. CONCLUSIONS

The paper defines an SCSAP scheme that solves the problem of small-grained access provision and storage rightness associated with the existing access control techniques. The first part of the SCSAP scheme involves the formation of hierarchical formation that fixes the appropriate access policies to the users; this improves the small-grained associated with the access policy. The deals with the achievement of storage correctness related to the files, and it is made through the usage of the token granting system. Use of token granting system improves the storage efficiency, security, and performance.

REFERENCES

[1] P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, "Cloud computing security issues in Infraformation as a service," International Journal of Advanced Research in Computer Science and Software Engineer in, vol. 2, no. 1, pp. 1–7, 2012.

[2] V. Bhangotra and A. Puri, "Enhancing cloud security by using hybrid encryption scheme," International Journal of Advanced Engineering Technology, vol. 6, no. 4, pp. 34–40, 2015.

[3] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute sets: A practically motivated enhancement to attribute based encryption," in Computer Security (ESORICS'09), pp. 587–604, Springer, 2009.

[4] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it plat forms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.

[5] Z. Cao, C. Mao, L. Liu, "Analysis of one secure anti collusion data sharing scheme for dynamic groups in the cloud," International Journal of Electronics and Information Engineering, vol. 5, no. 2, pp. 68–72, 2016.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for small-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98, 2006.

[7] W. Huang, A. Ganjali, B. H. Kim, S. Oh, and D. Lie, "The state of public infraformation as a service cloud security," ACM Computing Surveys, vol. 47, no. 4, pp. 68, 2015.

[8] N. Kaaniche, A. Boudguiga, and M. Laurent, "ID based cryptography for secure cloud data storage," in 2013 IEEE Sixth International Conference on Cloud Computing, 2013.

[9] R. KO and R. Choo, the Cloud Security Ecosystem: Technical, Legal, Business and Management Issues, Syngress, 2015.

[10] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity based encryption with outsourced revocation in cloud computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, 2015.

[11] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: cipher text policy attribute based sign encryption," Future Generation Computer Systems, vol. 52, pp. 67– 76, 2015.

[12] O. Manholes and P. Tyrv¨ainen, "Role of data communications in hybrid cloud costs," in 2011 37th IEEE EUROMICRO Conference on Software Engineering and Advanced Applications, pp. 138–145, 2011.

[13] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Proceeding of IEEE Information Security for South Africa (ISSA'10), pp. 1–7, 2010.

[14] B. D. Revathy, M. P. Ravishankar, and C. I. T. Ponnampet, "Enabling secure and efficient keyword ranked search over encrypted data in the cloud," 2015.

[15] P. Samarati and S. De C. Di Vimercati, Cloud security: Issues and concerns, Wiley, New York, 2016.

[16] J. Singh, "Cyber attacks in cloud computing: A case study," International Journal of Electronics and Information Engineering, vol. 1, no. 2, pp. 78–87, 2014.

[17] Z. Wan, J. Liu, and R. H. Deng, "Hasbe: A hierarchical attribute based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.

[18] C. Wang, S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[19] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," IEEE Network, vol. 24, no. 4, pp. 19–24, 2010.

[20] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[21] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute based encryption scheme in cloud computing," IEEE Transactions on Information Forensics and Security, vol.11, no.6, pp.1265–1277, 2016.

[22] H. Witti, C. Ghedira, E. Disson, and K. Boukadi, "Security governance in multicloud environment: A systematic mapping study," in 12th World Congress on Services (SERVICES'16), 2016.

[23] Y. Wu, Z. Wei, and R. Deng, "Attribute based access to scalable media in cloud assisted content sharing networks," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

[24] K. Yang and X. Jia, "Dacmacs: Effective data access control for multiauthority cloud storage systems," in Security for Cloud Storage Systems, pp. 59–83, Springer, 2014.

[25] L. Zhou, V. Varadharajan, and M. Hitchens, Achieving secure role based access control on encrypted data in cloud storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947–1960, 2013.

BIOGRAPHIES

Head of the Department (BCA), Dept of Computer Science and Application, D.K.M.College for Women (Autonomous), Vellore, Tamilnadu, India.

Research Scholar**,** Dept of Computer Science and Application, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.

Head of the Department (B.Sc)**,** Dept of Computer Science and Application, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.