ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Comprehensive and Comparative Analysis of Cryptographic Solutions in Cloud

P.Madhubala[1], Dr.P.Thangaraj[2]

Research Scholar, Department of Computer Science, Mother Theresa Women's University, Kodaikanal, TamilNadu, India[1]

Head of Department, Department of CSE, Bannari Amman Institute of Technology, Sathiyamangalam, TamilNadu, India[2].

ABSTRACT: Cloud computing has swiftly advanced a broadly adopted archetype for providing pay for use services over the global net services. The cloud computing resources are stored as a pool. The cloud service provider is the authorized person to maintain the data stored in cloud. Therefore the security and trust for data storage is dependent on the third-party provider. For the protective privacy of the deposited data, proper encryption is needed before uploading to the cloud. In this paper, we summarized the cryptographic techniques and investigate basic encryption schemes and Compare the basic security parameters of various existing data encryption schemes for data storage in cloud. Finally, we list the comparison relationships ofABE schemes by some criteria for cloud environments.

KEYWORDS: Cloud, Data, key, algorithm, Encryption

I. INTRODUCTION TO CRYPTOGRAPHY

The word is derived from the Greek crypto's, meaning hidden. Cryptography is a science of devising methods that allow information to be encrypted and sent in a secure from in such a way that the only person to able retrieve this information is the intended recipient. Encryption is based on algorithms that scramble information (Plaintext or Clear Text) into unreadable (Cipher Text) form. Decryption is the process of restoring the scrambled information to its original form. Cryptographic systems are used to provide privacy and authentication in computer and communication systems. Cryptography is the one of best way to protect data at rest as well as data at transit.

The data at rest can be encrypted in following four ways. They are encrypting 1) full disk level, 2) directory level,3) file level and 4)application level. The gravest part for implementation of any of these methods is managing key for data encryption and decryption. The common way to protect data in transit is to utilize encryption with authentication, which securely pass data to or from the cloud server [1].Cryptographic algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, and group of bits or letters) is mapped into another element and in transposition, the elements of the plaintext have simply been re-arranged in different order; their position with relation to each other have been changed.

A.TYPES OF CRYPTOGRAPHY

The cryptography can apply two types of encryption. Symmetric and Asymmetric Key Encryption.

SYMMETRIC-KEY ENCRYPTION:

A type of encryption where the same key is used to encrypt and decrypt the message. Symmetric key encryption is the one of the oldest methods of encryption in use in world today and is secure because the user must have the key to decrypt and read data. The encryption may use a stream cipher or block cipher based on the amount of data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

ASYMMETRIC-KEY ENCRYPTION:
A type of encryption where the different key is used to encrypt and decrypt the message.The encryption algorithms support compliance, protect the user against breach incidents, and secure information against advanced threatsthere are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc. are some symmetric algorithm. DES and AES are mostly used symmetric algorithms.DES is quite simple to implement then AES.

RSA and Diffie-Hellman Key Exchange are the asymmetric algorithms. In cloud computing both RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms. These algorithms maintains the confidentiality of data.

II. THE BASIC CLOUD IMPLEMENTATION MODEL

Basically, the service models of cloud is spread as ISP, Where I-Infrastructure as a Service , S-Software as a Service and P-Platform as a Service. And the deployment of a cloud is managed in-house (Private Cloud) or over a third-party location (Public Cloud). While, for various reasons, it is deployed as an integrated private-public cloud (Hybrid Cloud). A "Community Cloud" is a fourth type of cloud implementation models, where the infrastructure spreads over several organizations and is accessed by a specific community. The different cloud implementation models are shown in Figure 1.

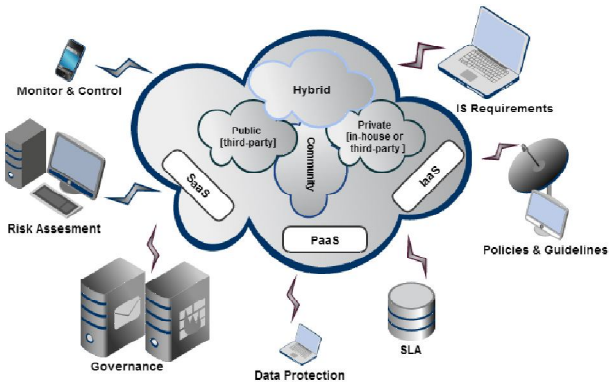

Figure 1. Cloud implementation model

III. CLOUD ENCRYPTION MODEL

Cloud encryption is a service offered by cloud storage providers whereby data, or text, is transformed using encryption algorithms and is then placed on a storage cloud. Cloud encryption is the transformation of a cloud service customer's data into ciphertext.

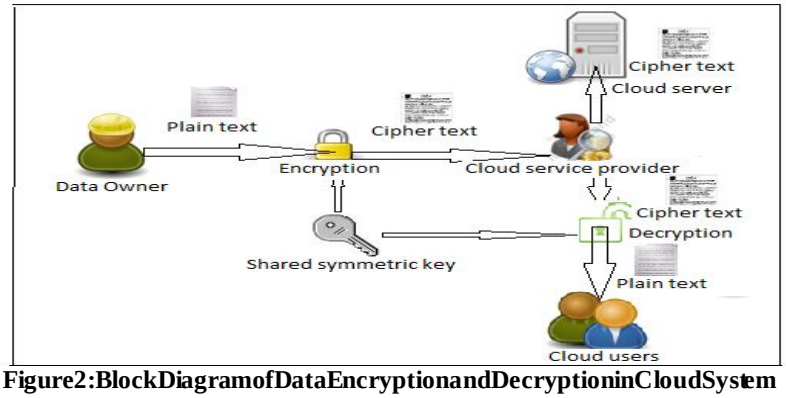

Figure2:BlockDiagramofDataEncryptionandDecryptioninCloudSystem

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Cloud encryption is almost identical to in-house encryption with one important difference -- the cloud customer must take time to learn about the provider's policies and procedures for encryption and encryption key management. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted.Because encryption consumes more processor overhead, many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers. At this point in time, having the provider encrypt a customer's entire database can become so expensive that it may make more sense to store the data in-house or encrypt the data before sending it to the cloud.

IV. RELATED WORK

The related work that containing the study of various cryptographic algorithms. These algorithms ensure the high level confidentiality and authentication. A cryptographic algorithm is cautious to be computationally secured if it cannot be cracked with standard resources. An effectual cryptosystem can create best possible results if key size is comparable to the size of the packet to be transmitted over the network. Fatemimoghaddam et al. In [7], discussed the performance of s ix differ rent symmetric key RSA data encryption algorithm in c loud computing environment. They have proposed two individual cloud servers; one for data s server and other for key cloud server and the data encryption and decryption process at the client s ide. The major demerit of this method is to maintaining two separate servers for data security in cloud, which leads a more storage and computation overheads .

Table 1: Symmetric VS Asymmetric algorithms

Issues	**DES**	**AES**	**RSA**	**ECC**
Provider	IBM 75	Rijman, Joan	Rivest, Shamir	Neal Koblitz,Vic
Key Length	56-bits	128,192, and256	Based on	135bits
BlockSize	64-bits	128bits	Variant	Variant
Security Level	Not enough	Excellent	Good	Less
Executionn Time	Slow	More Fast	Slowes t	Fastest

V. COMPARATIVE INVESTIGATIONS ON SOLUTIONS BY DIFFERENT AUTHORS

There have been a number of analyses of security solutions applied for enhancing security and privacy in the Cloud. Xiao and Xiao [5] identifies the five concerns of Cloud computing; confidentiality, integrity, availability, accountability, and privacy and thoroughly reviews the threats to each of the concerns as well as defense strategies. Chen and Zhao [6] outline the requirements for achieving privacy and security in the Cloud and also briefly outline the requirements for secure data sharing in the Cloud. Zhou [7] provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud. Wang et al. [8] explored factors that affect managing information security in Cloud computing. It explains the necessary security needs for enterprises to understand the dynamics of information security in the Cloud. Wang [9] carried out a study on the privacy and security compliance of Software-As-A-Service (SaaS) among enterprises through pilot testing privacy/security compliance. They then carry out analysis work on the measurements to check whether SaaS complies with privacy and security standards.

The method does not however take into account other Cloud models such as Platform- As-A-Service (PaaS) and in particular Infrastructure-As-A-Service (IaaS), as needed for data sharing. Oza et al. [10] carried out a survey on a number of users to determine the user experience of Cloud computing and found that the main issue of all users was trust and how to choose between different Cloud Service Providers. This states, "Although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern." Thereare many examples of insider attacks such as Google Docs containing a flaw that inadvertently shared user documents,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

MediaMax going out of business in 2008 after losing 45 % of stored client data due to administrator error, Salesforce.com leaking a customer list and falling victim to phishing attacks on a number of occasions.

Following table summarizes the comparative analysis on the existing security solutions for secured data sharing in cloud introduced by various researchers.

Table 2: Table with comparative security values based on various authors

Authors	Cloud Security	Data Sharing	Threats	Defense Strategies	Storage Overhead	Key Size
Zhibin Zhou	T	F	T	Y	High	Linear
XiaoanXiao	T	F	T	T	Less	Linear
ChenandZhao	T	T	T	F	Average	
Zhou	T	F	T	T	High	constant
Wangetal.	T	F	F	T	Low	Linear
Wang	T	F	F	T	High	Constant
Ozaetal	T	F	Y	F	High	Linera
SaradhyandMuralidhar	F	F	F	F	HIgh	Constant
Butler	F	T	T	F	Low	Consatant
Mitchley	F	T	T	F	Avearage	Linear
Feldmanetal	F	T	F	F	Avearage	Linear
Geoghegan	F	T	F	F	Low	Constant
SahafizadehandParsa	F	T	F	F	High	Linear

VI. ANALYSIS OF ATTRIBUTE ENCRYPTION STORAGE SCHEMES

Attribute-Based Encryption (ABE) makes the user and data attributes as the major components for generating keys while the data is encrypted. Attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encryptor determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is more appropriate to the data sharing system because, it puts the access policy decisions in the hands of the data owners. The access policy can be categorized as either key-policy or ciphertext-policy. The key-policy isthe access structure on the user's private key, and the cipher text-policy is the access structure on the cipher text. And the access structure can also be categorized aseither monotonic or non-monotonic one. They have been designed the data decryption algorithm based on the user requested attributes of the outs sourced encrypted data. Using ABE schemes can have the following two advantages: (1) to reduce the communication overhead of the Internet, and (2) to provide a fine-grained access control.

A.Key Policy Attribute Based Encryption (KP-ABE)

It is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree Structure the secret key of the user is defined. Ciphertext are labeled with sets of attributes and private keys are associated with monotonic access structures that control which ciphertexta user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications.

B.Cipher Text Policy Attribute Based Encryption (CP-ABE)

Another modified form of ABE called CP-ABE introduced by Sahai. In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

access policy associated with the ciphertext. CP-ABE works in the reverse way of KP-ABE. The access structure of this scheme or algorithm, it inherit the same method which was used in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data; it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is similar to the traditional access control schemes. The encryptor who specifies the threshold access structure for his interested attributes while encrypting a message.

It improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt. It can support the access control in the real environment. In addition, the user's private key is in this scheme, a combination of a set of attributes, so an user only use this set of attributes to satisfy the access structure in the encrypted data.

Drawbacks of the most existing CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP- ABE has limitations in terms of specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so the users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. After that ciphertext-policy attribute-set-based-encryption (CP-ASBE or ASBE for short) is introduced by Bobba, Waters et al ASBE is an extended form of CP-ABE. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. The CP-ASBE consists of recursive set of attributes. The challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from multiple keys.

C. Attribute-based Encryption Scheme with Non- Monotonic Access Structures

Previous ABE schemes were limited to expressing only monotonic access structures and there is no satisfactory method to represent negative constraints in a key's access formula. Ostrovsky et al. proposed an attribute-based encryption with non-monotonic access structure in 2007.Non-monotonic access structure can use the negative word to describe every attributes in the message, but the monotonic access structure cannot. It enables Non-monotonic policy, i.e. policy with negative attributes.

The problem with Attribute-based Encryption Scheme with Non- Monotonic Access Structures is that there are many negative attributes in the encrypted data, but they don't relate to the encrypted data. It means that each attribute adds a negative word to describe it, but these are useless for decrypting the encrypted data. It can cause the encrypteddata overhead becoming huge. It is inefficient and complex each ciphertext needs to be encrypted with d attributes, where d is a system-wise constant.

D. Hierarchical attribute-based Encryption

This scheme Hierarchical attribute-based encryption (HABE) is derived by Wang et al The HABE model consists of a root master (RM) that corresponds to the third trusted party (TTP),multiple domain masters (DMs) in which the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. The following gives the comparison of each schemes in the attribute base dencryption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

TABLE 3: COMPARISON OF ABE SCHEMES

Techniques/ Parameter	ABE	KP-ABE	CP-ABE	HABE	MA-ABE
Fine grained Access Control	Low	Low, High if there is reencryption technique	Average Realization of complex Access Control	Good Access control	Better Access control
Efficiency	Average	Average, High for broadcast type system	Average, Not efficient for modern enterprise environments	Flexible	Scalable
Computational Overhead	High	Most of computational overheads	Average computational overheads	Some of overhead	Average
Collusion resistant	Average	good	good	good	High collusion resistant

The first Attribute based algorithm was proposed by Sahai and Waters in 2005 Theyadopted Fuzzy Identity-Based Encryption.They introduced the Principal concept of the attribute-based encryption scheme based on public key cryptography. They first presented Fuzzy Identity-Based Encryption in which identities are used as a set of descriptive attributes. Fuzzy IBE can be used for an application as an attribute based encryption. In this scheme, each user is recognized by a set of attributes, and some function of this attributes is used to define decryption capability for each ciphertext. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

In 2006 M. Pirretti, P. Traynor, P. McDaniel, and B. Waters proposed Secure attribute-based systems. Theyproposed an implementation of the ABE encryption system with more complex access policy with (AND, OR gate). This work also demonstrated different applications of attribute-based encryption schemes and addressed several benefits of data encryption and the limitations. Jing-Jang Hwang et alhas proposed a new model for c loud computing for data security using data encryption and decryption algorithms . In thismethod cloud service provider is res pons bile for storageof data and data encryption/decryptionprocess, which takes more computational,costs.One of the main efficiency drawbacks of this method is, cloud service provider has more calculation and storage overhead for verification of user attributes with the outsourced encrypted data. While introducing third party auditor we can reduces the storage, computation, and communicational overheads of the cloud server, which improves the efficiency of the cloud data s storage.This work also demonstrated different applications of attribute-based encryption schemes and addressed severalpractical notions such as key-revocation and optimization. However, this task isterminated after the proposal of KP- ABE and CP-ABE, which is more flexible and efficient. In the same year, Goyal et al. proposed a key-policy attribute-based encryption (KP-ABE) scheme. Fine grained access control provided by KP-ABE as compared with classical model.

In 2007 Bethencourt et al.Proposeda ciphertext- policy attribute based (CP-ABE) scheme. Data owner only trusts the key issuer as CP-ABE scheme addresses theproblem of KP-ABE. Both KP-ABE and CP-ABE are ableto enforce general access policies that can be described by a monotone access structure. Moreover, Muller proposed an distributedattribute-based encryption scheme in 2008; Yu e. proposed a fine-grained data access control encryption scheme ; Tang proposed a Verifiable attribute based encryption scheme . Ostrovsky et al. proposed an enhanced ABE scheme which supports non-monotone access structures [8].

In 2008 Muller et al. proposed an distributed attribute-based encryption scheme.Wang et alproposed a hierarchical attribute-based encryption scheme(HABE) [10] in 2010. This algorithm integrates properties in both an IBE(hierarchical identity based encryption) model and a CP-ABE model. There after introduce a MA-ABE(multi-authorities ABE)schemes that use multiple parties to distribute attributes for users.Attribute-based encryptionschemes can be further categorized as either monotonic or non-monotonic based on their type of access structure.Comparison of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

communication overhead and Storage overhead in different transmission encryption schemes andgroup key management schemes.

Table 4: N : the number of group members; l: the number of leaving members; t: maximum number of colluding users to compromise the ciphertext.

Scheme	CommunicationOverhead		StorageOverhead	
	singlereceiver	multiplereceivers	Center	User
ABBE	$O(1)$	$\approx O(\log N)$	N/A	$O(\log N+m)$
Subset-Diff	$O(t^2 \cdot log^2 t \cdot \log N)$	$O(t^2 \cdot log^2 t \cdot \log N)$	$O(N)$	$O(t\log t\log N)$
BGW1	$O(1)$	$O(1)$	N/A	$O(N)$
BGW2	$O(N2)$	$O(N2)$	N/A	$O(N2)$
NNL1	N/A	$O(t\log(N/t))$	N/A	$O(\log N)$
NNL2	N/A	$O(t)$	N/A	$O(\log^2 N)$
DPP1	O(1)	$O(1)$	N/A	$O(N)$
DPP2	N/A	$O(t)$	N/A	$O(1)$
BW	1	1	N/A	1
LT	N/A	$O(t)$	N/A	$O(\log N)$
ACP	$O(N)$	$O(N)$	$O(N)$	$O(1)$
Flat-Table	$O(\log N)$	$\approx O(\log N)$	$O(\log N)/O(N)$	$O(\log N)$
Flat-Table-ABE	$O(\log N)$	$\approx O(\log^2 N)$	$O(\log N)/O(N)$	$O(\log N)$
Non-Flat-Table-Tree	$O(\log N)$	$O(l \cdot \log N)$	$O(N)$	$O(\log N)$

VII. CONCLUSION

In this paper, we summarized cryptographic methods and analyzeddifferent symmetric and asymmetric attribute-based encryption schemes: ABE,KP-ABE,CP-ABE, ABE with non-monotonic access structure, HABE and MA-ABE. The main access polices are KP-ABE and CP-ABE, further schemes are obtained based on these policies. Based on their type of access structure the schemes are categorize das either monotoni cornon-monotonic. For many reasons, including the reduction of capital expenditures, organizations need to con- sider utilizing cloud services as an essential part of their foundations. Never the less, various challenges are avoiding the accomplishment of gigantic arrangement and recognition levels.The main drawback of the existing cloud service implementations is their inability to provide high security level.To have better utilization of cloud services many issues need to be enhanced in a way for guaranteeing high level of security, confidentiality,authenticity, integration, agility,scalability andtrust.

REFERENCES

1.J R Winkler, Securing the Cloud:Cloud ComputingSecurity Techniques and Tactics , Elsevier Inc.,USA, 2011.
2. D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592. http://www.sciencedirect.com/science/article/pii/S0167739X10002554http://dx.doi.org/10.1016/j.future.2010.12.006
3.Communications andNetwork, 2014,6,15-21PublishedOnlineFebruary2014(http://www.scirp.org/journal/cn)
http://dx.doi.org/10.4236/cn.2014.61003
4.InternationalJournalOfEngineering AndComputerScienceISSN:2319-7242Volume3 Issue4 April, 2014 PageNo.5215-5223
5.XiaoZ,XiaoY(2012)Securityandprivacyincloudcomputing.IEEECommonSurveysTutorials99:1–17
6.ChenD,ZhaoH(2012)Datasecurityandprivacyprotectionissuesincloudcomputing.Inter-
nationalconferenceoncomputerscienceandelectronics,engineering,pp647–651.
7. ZhouM(2010)Securityand privacyin thecloud:a survey.Sixthinternationalconferenceon semanticsknowledgeandgrid(SKG)2010:105–112
8.WangJ,LiuC,LinGTR(2011)Howtomanageinformationsecurityincloud,computing,pp1405–1410.
9.WangY(2011)TheroleofSaaSprivacyandsecuritycomplianceforcontinuedSaaSuse.Inter-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

nationalconferenceonnetworkedcomputingandadvancedinformationmanagement(NCM)2011:303–306
10.OzaN,KarppinenK,SavolaR(2010)Userexperience andsecurityinthecloud-Anempir- icalstudyinthefinnish cloudconsortium.IEEEsecondinternationalconferenceoncloud computingtechnologyandscience(CloudCom)2010:621–628
11.SarathyR,MuralidharK(2006)Secureandusefuldatasharing.DecisSupportSyst204–220.
12. ButlerDDatasharingthreatensprivacy,vol449(7163).NaturePublishing,Group,pp644–645.
13. MitchleyM(2006)Datasharing:progressornot?Credit,Manage10–11.
14. FeldmanL,PatelD,OrtmannL,RobinsonK,PopovicT(2012)Educatingforthefuture:anotherimportantbenefitofdatasharing.Lancet1877–1878.
15.Jing-Jang Hwang, Taoyuan, aiwan,Yi-Chang Hsu, Chien-HsingWu, ABusinessModelforCloudComputingBasedonaSeparate EncryptionandDecryption Service, in InternationalConferenceon InformationScienceand Applications(ICISA),pages1-7,2011.
16.FatemiMoghaddamF,KarimiO,AlrashdanM T, A ComparativeStudyofApplying Real-TimeEncryptioninCloud ComputingEnvironments, *inIEEE2nd International Conference onCloudNetworking(CloudNet),pages185-189*,2013.
17.Qin Liu,Tan CC,JieWu, GuojunWang, Reliable Re- Encryption in Unreliable Clouds,*in IEEE International Conferenceon Global Telecommunications(GLOBECOM)*,pages1-5,2011.
18.J.Katz, A.Sahai, and B. Waters.Predicateencryptionsupportingdisjunctions,polynomialequations,and inner products.*AdvancesinCryptology-EUROCRYPT*,4965:146–162,2008.
19.J.Bethencourt,A.Sahai, and B. Waters.Ciphertext-PolicyAttribute-BasedEncryption.*Proceedingsofthe 28th IEEESymposiumonSecurityandPrivacy (Oakland)*,2007. Pages:195-203
20. D.BonehandB.Waters.Conjunctive,subset,and rangequeries onencrypteddata.*TheoryofCryptography*,pages535–554,2007.
21. WangJ,LiuC,LinGTR(2011)Howtomanageinformationsecurityincloud,computing,pp1405–1410.
22.angY(2011)TheroleofSaaSprivacyandsecuritycomplianceforcontinuedSaaSuse.Internationalconferenceonnetworkedcomputingandadvancedinformationmanagement(NCM)2011:303–306
23.M.Armbrust,A.Fox,R.Grith,A.D.Joseph,R.Katz,A.Konwinski,G.Lee,D.Patterson,A.Rabkin,I.Stoicaand M.Zaharia,"AViewofCloudComputing,"*Communica- tions of the ACM*,Vol.53,No. 4,2010,pp.50-58. http://dx.doi.org/10.1145/1721654.1721672
24.Dr.L.Arockiam,S.Monikandan,DataSecurityandPrivacyinCloudStorageusingHybrid SymmetricEncryptionAlgorithm,InternationalJournalofAdvancedResearchinComputerandCommunicationEngineeringVol.2, Issue 8, August2013page .3064-3070
25. Cloud Security Solutions: Comparison of Various Security Algorithms, International l Journal of Advanced Research in Computer Sbcience and Software Engineering 4(4), Volume4, Issue4,April2014 .page1146-1148.

BIOGRAPHY

P.Madhubala MCA, MPhil is a Research Scholar in Computer Science, doing PhD in Mother Teresa Women's University and working as Assistant Professor Research Department of Computer Science in Don Bosco College, Dharmapuri,TN. She shows her sense of gratitude to DON BOSCO COLLEGE, Dharmapuri for their support and encouragement and MOTHER THERESA WOMEN'S UNIVERSITY, Kodaikanal for providing the opportunity to carry out the research work in Cloud Computing. She also like to thank her Research Supervisor Dr.P.Thangaraj for his guidance and valuable suggestions.

Dr.P.Thangaraj is Head of the Department-CSE in Bannari Amman Institute of Technology, Sathiya Mangalam,TN. He Has Published more than 40 journals and attended many conferences. His areas of research interests are Soft computing, Fuzzy Logic Wireless Sensor networks and Cloud Computing.