Research Study of Techniques for Securing Cloud

Miss. Pooja D.Bardiya, Prof.Mr.P.L.Ramteke

***Abstract*-- we have proposed this research study paper on the security issues in cloud computing as cloud computing will prove very attractive to the enterprise IT world and specifically to IT service providers primarily due to the infinite opportunities around innovative business models and it has proven to some extend itself as a emerging technology. Where information storage and access is the first prime importance in the corporate world, there are many researchers who have made the study about the security threats in cloud computing. Here we have proposed this paper about research study of how the security issues can be solved when user's identity, access rights and attributes is concerned. So that we can further develop a model that do not consists of issues like revocation ,less flexibility , complexity, large latency etc .here we have have made deep research study various techniques for securing cloud thorough three important aspects as mentioned above .**

***Index terms*-- Cloud Computing, Identity-Based Cryptography, Multi-authority ABE, Ciphertext Attribute Based Encryption, Identity and Access rights.**

I.INTRODUCTION

Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet.

Several trends [2] are opening up the era of Cloud computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale.

The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management.

***Miss.Pooja D.Bardiya**, Computer Science &Information Technology, S.G.B.A.U/ H.V.P.M College of Engineering,Amravati,India.*

***Prof .P.L.Ramteke,** Computer Science &Information Technology, S.G.B.A.U/ H.V.P.M College of Engineering, Amravati, India.*

We live in a more connected and fast-moving world than ever before. While our growing interconnectedness brings many benefits, it also means greater vulnerability and a heightened sensitivity to risk. Increasingly we look to technology to support both our personal and professional lives. As individuals, we expect instantaneous and ubiquitous access to communications, data, content, and applications at the same time; we expect constant availability and end-to-end security.

Cloud encompasses several variations of service models (i.e., IaaS, PaaS, and SaaS) and deployment models (i.e., private, public, hybrid, and community clouds) Cloud is not a "one-size-fits-all" proposition—the right approach depends on your organization's needs and priorities. Different service and deployment models can be adopted to match the requirements of different types of workloads from across the business Service providers must be prepared to address customer concerns ranging from policy compliance to end-to-end security to quality of service management to technical customization. They must be able to deliver a range of functionality, service levels, and payment, models.

In general, important requirements of cloud clients are that their data is processed in a confidential way (confidentiality), and that their data and computation was Processed in the expected way and has not been tampered with (integrity and verifiability).

Cloud computing model uses virtual machines. This enables the cloud service provider (CSP) to share the cloud infrastructure located in a datacenter between multiple customers and cloud computing services [4]. The customer does not need to maintain servers, train IT employees or even purchase software licenses[5]. Hence, the customer has transparency. This leads to lower cost in many things that are usually required by users such as management, training, power consumption, infrastructure maintenance, and storage space. Also, cloud computing can offer a high security for datacenters located in secret and well protected places.

ISSN: 2278 – 1323

Furthermore, cloud computing increases scalability (if the customer demand is increased then computer capability is responded and can grow), expediency in new service roll out, availability (a failure of one component will not disconnect all components), and mobility [5]. Cloud computing increases the flexibility of organizations due to information sharing and collaboration (multitenancy).The characteristics of clouds include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service[6].

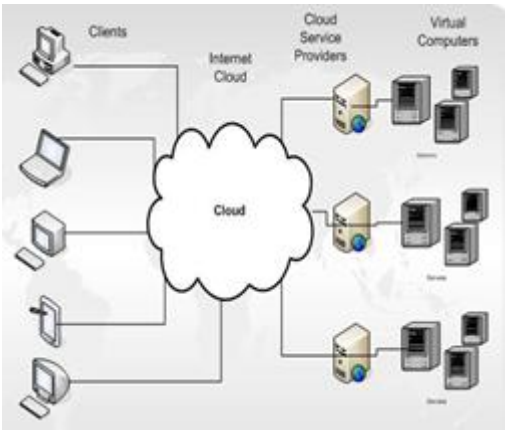

Fig 1: clients and and virtual computers connected by Internet cloud through service provider

The most important advantages of cloud computing can be summarized as follows [7]:

- Cloud computing is easy to be used, and do not need high quality equipment from users.
- The user that use cloud computing do not need to worry about the problems such as data loss or virus, because cloud computing provides dependable and secure data storage center.
- Cloud computing can realize data sharing between different equipment.
- Cloud provides nearly infinite possibilities for users to use internet

Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing. The boom in cloud computing has brought lots of security challenges for the consumers and service providers.

While sharing IT infrastructure in cloud computing is cost-efficient and provides more flexibility for the clients, it introduces security risks organizations have to deal with in order to isolate their data from other cloud clients and to fulfill confidentiality and integrity demands. Moreover, since the IT infrastructure is now under control of the cloud provider, the customer has not only to trust the security mechanisms and configuration of the cloud provider, but also the cloud provider itself.

There are various papers been published when the cloud access storage and security is concerned .In this paper we are trying to make a reaserach study how the drawbacks of cloud related to how authentication authorization and access can be achieved so that they can be cemented.We are also making a research study of what are the advancement scope that can be made in cloud so that even small organization can make them benefited with little investment and more output[2].

Encryption is a commonly adopted approach to protect the confidentiality of the data. Encryption alone, however, is not sufficient as organizations often have to enforce fine-grained access control on the data. Such control is often based on the attributes of users, referred to as identity attributes, such as the roles of users in the organization, projects on which users are working and so forth. These systems, in general, are called attribute-based systems. Therefore, an important requirement is to support fine-grained access control, based on policies specified using identity attributes, over encrypted data.

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information.

Using ABE, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys. Only when the users have matching set of attributes, can they decrypt the information stored in the cloud. ABS can be combined with ABE to achieve authenticated access control without disclosing the identity of the user to the cloud.

Cloud Computing systems includes a large amount of various computing resources, most data and software reside on the Internet, and it provide digital identity for users to access their services, This requires more flexibility for the users. Using cloud computing service, users can store their critical data in servers and can access their data anywhere and anytime via the Internet and they should not worry about system attacks, breakdown, or disk faults [3].As there are many vulnerabilities that need to take care of them in cloud computing, this brings some challenges for the system, especially security and privacy.

In this paper we have made the deep research on the key words mentioned .security is the only issue when the cloud computing is actually used .cloud computing is the emerging technology which stands alone for its features and drawbacks .how the cloud is being evolved and used

ISSN: 2278 – 1323

by many small and big organization like amazon, google facbook etc for its application and benefited .

Cloud encompasses several variations of service models (i.e., IaaS, PaaS, and SaaS) and deployment models (i.e., private, public, hybrid, and community clouds) Cloud is not a "one-size-fits-all" proposition—the right approach depends on your organization's needs and priorities. Different service and deployment models can be adopted to match the requirements of different types of workloads from across the business.

II. IDENTITY-BASED CRYPTOGRAPHY

Initially we studied encryption is one of the security ways in order to hide the information sent and received on the network .we found that these algorithms can be used to hide the identity of the user in [7][8][9] but that was the simple way of cryptography . In this the combination of public key and the private key and this private key is generated by the PKG(private key generator). How one securely and efficiently obtains this private key is essential to the security of the supported system

Independent of cloud computing, a variant of traditional public key technologies called Identity-Based Cryptography (IBC) [6, 7] has recently received considerable attention. Through IBC, an identifier which represents a user can be transformed into his public key and used on-the-fly without any authenticity check. The potential of IBC to provide greater flexibility to entities within a security infrastructure and its certificate-free approach may well match the dynamic qualities of cloud environment.

Identity-Based Cryptography (IBC) is in a very quick development [20]. Identity-Based Encryption (IBE)provides a public key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number . The corresponding private key can only be generated by a Private Key Generator (PKG) who has knowledge of a master secret. Using this construct, anyone can encrypt messages or verify signatures without prior key distribution beyond the dissemination of public parameters and the public key "strings." This is useful where the deployment of a traditional certificate authority-based PKI is inconvenient or infeasible, as IBE-based systems do not require certificate management, eliminating the need for certificate lookups and complex certificate revocation schemes. A central operational consideration of Identity-Based Cryptography is that private keys must be obtained from the PKG. How one securely and efficiently obtains this private key is essential to the security of the supported system.

After the identity based cryptography (IBC) Being developed to identity based encryption (IBE)which offered the security better then IBC .after that it was found that attributes sent by the user stored at the cloud can be used for the malpractises .now the next research was to encrypt the attributes stored and it was developed to attribute based encryption .

Attribute based encryption is a type of encryption in which the secret key of a user and the ciphertext are dependent upon the attributes like name, country, address etc.In such a system the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext .a crucial security aspect of attiribute –based encryption is collusion resistant .an adversary that holds mulptiple keys should only be able to access data if at least one individual key grants .the concept of attribute was frist purposed by Amit Sahai and Brent Watersand later by V ipul goyal ,Omkant Pandey ,amit sahai ,and Brent waters .

Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. In traditional public key encryption or identity-based encryption systems, encrypted data is targeted for decryption by a single known user. Unfortunately, this functionality lacks the expressiveness needed for more advanced data sharing. To address these emerging needs, Sahai and Waters introduced the concept of attribute-based encryption (ABE).

III. MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION

Identity based encryption(IBE), introduced by Shamir [Sha85], is a variant of encryption which allows users to use any string as their public key (for example, an email address). This means that the sender can send messages knowing only the recipient's identity (or email address), thus eliminating the need for a sep- arate infrastructure to distribute public keys. The first IBE systems were given by Boneh and Franklin [BF01] and Cocks [Coc01].but when IBE scheme is concerned ,the user must go to to the trusted party for proving his/her identity and give his certain set of attributes in order to obtain secret key corresponding to each of those attributes that will be used to decrypt the message.

In an identity based encryption scheme[10], each user is identified by a unique identity string. In contrast ABE is the Scheme where the user is identified by a set of attributes and then some functions are used on those attributes to encrypt those attribute and decrypt those cipher text. Initially single authority attribute encryption scheme was introduced. The most challenging aspect of a single authority ABE scheme is preventing collusion and that encouraged for the construction in which multiple authorities attribute encryption. Instead of encrypting to individual users, in ABE system, one can embed an access policy into the ciphertext or decryption key.

ISSN: 2278 – 1323

There can come a situation of collusion in which two user having two out of three attributes can combine their keys and decrypt the cipher text in the single authority ABE while in multiauthority ABE Sahai and Waters describe a scheme (from here on referred to as SW) in which a sender can encrypt a message specifying an attribute set and a number d so that only a recipient who has at least d of the given attributes can decrypt the message. Thus, their scheme allows the sender to encrypt a message for more than one recipient, and to specify who should be able to decrypt, using attributes alone. Could be formed simply by letting each authority run its own copy of SW and then combining the results. However, here we once again run into the problem of collusion.

The solution to this problem is given in this paper. [11] This paper made a scheme that scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. We give an efficient scheme for multiauthority attribute based encryption. We allow the sender to specify for each authority k a set of attributes monitored by that authority and a number dk so that the message can be decrypted only by a user who has at least dk of the given attributes from every authority. We allow any number of attribute authorities to be corrupted, and guarantee the security of encryption as long as the required attributes cannot be obtained exclusively from those authorities and the trusted authority remains honest.

ABE can be viewed as an extension of the notion of identity-based encryption in which user identity is generalized to a set of descriptive attributes instead of a single string specifying the user identity. Compared with identity-based encryption, ABE has significant advantage as it achieves flexible one-to-many encryption instead of one-to-one; it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control.

Then the further study found that user who has to be recalled or terminated the previously granted power or accessibility must be the prime importance when the security is concerned. It is nothing but the revocation .next the study was made on revocation of the invalid users or the person who is no longer allowed to access the data. The solution to this problem led to model of CP-ABE and KP-ABE.

In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of descriptive attributes, while user's private key is issued by the trusted attribute authority captures an policy (also called the access structure) that specifies which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast . For example, in a secure forensic analysis system, audit log entries could be annotated with attributes such as the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action. While a forensic analyst charged with some investigation would be issued a private key that associated with a particular access structure. The private key would only open audit log records whose attributes satisfied the access policy associated with the private key. The first KP-ABE construction was provided by Goyal et al. [5], which was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. The system was proved selectively secure under the Bilinear Diffie-Hellman assumption. Later, Ostrovsky et al. [6] proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including nonmonotone ones, by integrating revocation schemes into the Goyal et al. KP-ABE scheme.

IV. CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION

Revocation is a vital open problem in almost every cryptosystem dealing with malicious behaviors. It is the act in which the user can access the data even if he/she is not authorized to access .it shoud be ensured that users must not be able to access data ,even if they posses matching set of attributes .

In ciphertext policy attribute based encryption, unlike traditional public key cryptosystem different users may hold the same functional secret keys related with the same attribute set leading to additional difficulties in designing revocation mechanism. Ciphertext Policy Attribute based Encryption (CP-ABE), similar with role-based access control system, can be widely applied to realize access control in many applications including medical systems and education systems.

In the traditional CP-ABE scheme, once users obtain the credentials from a system manager at the beginning of setup phase, the access ability is always valid for those who may even break the confidential rules by abusing these private information. Upon detecting those malicious adversaries, without any revocation mechanism embedded, the system manager has to rebuild up the whole system.

Several factor s to be considered when designing the revocation in CP-ABE:

- System manager only associates user secret keys with different sets of attributes instead of individual characteristics. The fuzzy identities therefore encumber the system's revocation on one specified user;
- Users' individuality are taken place by several common attributes, and thus revocation on attributes or attribute sets can not accurately exclude the users with misbehaviors.

ISSN: 2278 – 1323

- System must be secure against collusion attack from revoked users even though they share some common attributes with non-revoked users.

For example, the sensitive medical records, tightly related to patients' privacy, must be accessed only if the users are authorized with patients' consent. The CP-ABE scheme deals with those situations, by encrypting the target information with expressive access policies, such as "Medicine" and "Physician". Another example can be solutions of exams in the education online system also should be only read by professors or specified teaching assistants "Professor" or ("Computer Science" and "Teaching Assistant").

Cloud computing has the features of low cost and on – demand service over the network. Though it has features but there is the risk as lots of highly confidential data is stored on cloud which is sensitive and they must be protected from the unauthorized person. Protecting personal privacy and information in order to secure the data on cloud .one of the way to secure the data and maintain the confidentiality and integrity f the data user's identity and access rights must be preserved. The unauthorized uers must be strictly be kept away from the identity and access. Managing user's identity and providing adequate privacy and protection will be a great challenge because most providers are depending on different information systems to provide their services.

V. IDENTITY AND ACCESS RIGHTS

This paper [5, 6] has proposed the solution to issue of identity and access rights of users in cloud environment. Our proposed system that is based on combined techniques of Identity-Based cryptography (IBC) and mediated cryptography (mediated RSA) is introduced.

The initial step to trap ones data is to know the identity and its other attributes. The main attributes related to the users is his/her presence and location of access. Presence is associated with the real-time communication systems such as Instant Message (IM) and Voice over IP (VoIP). Such systems usually provide descriptions about users' status during or after the communication, whether they are idle or active, online or offline, etc. Geographic location can be specified by IP address of the entity.

users access rights can be preserved by means of Authorization, Authentication, and Auditing. The trust boundary is secured via network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication. The organization's trust boundary with cloud computing will become dynamic and the application, system, and network boundary of an organization will extend into the service provider domain. Thus, application security and user access controls must compensate for the loss of network control and to strengthen risk assurance.

Some of the benefits for Identity and access rights are :

- Improved controls by reduced security risk.
- Providing transparency by eased regulatory compliance.
- Reduced administrative expenses and improved efficiency.
- Improved IT agility through automated security processes.

We will see the way for securing Identity and access rights:

1) Trusted Generator Center:

- Generating a "master" private key and corresponding "master" public key (generating public parameters- PP), dividing the private key into two parts, and giving one for user and other for the SEM.
- GC will make the "master" public key public for all the interested users. Any user can use this "master" public key and the identity of a user (identity must be unique) to create the private key of this user
- GC will use the identity and the "master" private key to generate the private key for this user.
- The user needs session key to exchange the key information secretly and secure channels to transmit private keys.

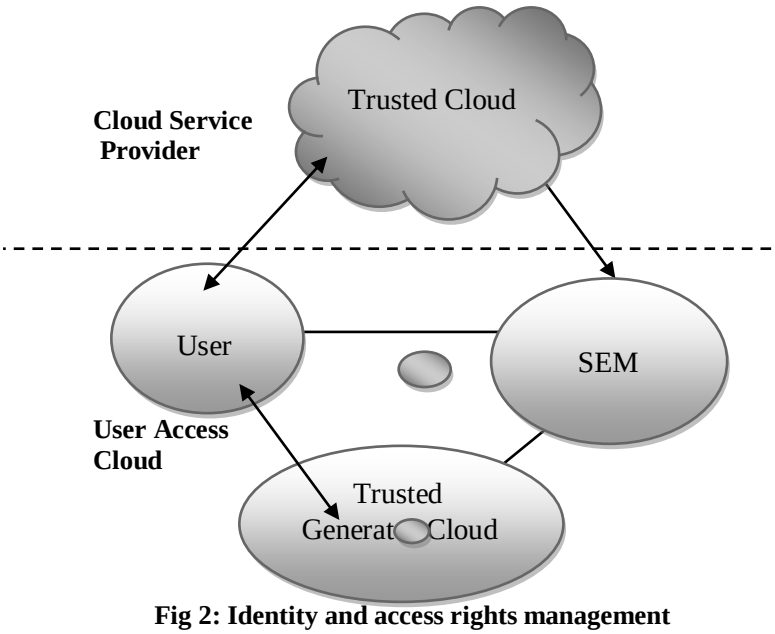

Fig 2: Identity and access rights management

2) Security Mediated Center (SEM):

- SEM is the second part of the system which will have the half of the user's private key (PRSEM).
- SEM takes all the halves of the users' private keys from GC and stores them in the database with other information of user.
- SEM have many advantages such as:

ISSN: 2278 – 1323

(i) The full operation cannot be accomplished without acceptance of SEM because it has the half of user private key,
(ii) It manages all user activities such as (request, timestamp, authorization, etc.), and
(iii) It sends to TC and user the half of user private key (PRSEM).
(iv) SEM adds a time period to the identifier of the user in order to solve the revocation problem.

- Revocation problems may occur because all the users in the system use some unique identifiers (such as email address, user's name, address, etc.) as their public keys. Hence, SEM adds some time period to the identifier of the user to control public keys of users and prevent (or reduce) the unauthorized usage of identities by an attacker if the attacker success to get user's private key.

3) User:

- The third part of the proposed system is the user which should download the parameters before requesting his private key from GC in order to use the system.
- GC will provide the user with the half of private key of him/her (PRu). The SEM must provide the other half of user private key (PRSEM).
- Then the user sends user private key (PRu) and ID to Trusted cloud (TC).
- TC combines the two halves of private key (PRSEM and PRu) by using a suitable algorithm and generates the private key.
- TC can use symmetric cryptography method to encrypt the data (such as AES) and send it to client

4) The Trusted Cloud (TC):

- TC is used to manage virtualization, federation, and update as shown in Fig 2.
- TC also manages all cloud server providers (CSPs). For example, if a user using Google CSP want to use another cloud provider (such as Amazon) of different infrastructure, then the user does not need to repeat the whole registration procedure. Using identity federation can increase the security of network since it only requires a user to identify and authenticate himself/herself to the system for one time and this identity information can be used in different networks.
- Using identity federation in the cloud enables users from different clouds to use a federated identification to identify themselves. Updates are done by TC to add new CSP or to add new branch for old CSP.

VI. CONCLUSION

In this paper we have made a deep research on one of the serious security defect cloud computing is identity access and attributes of user .these three parts are the key parts or we can say the first layer for malicious activities. Initially we studied cloud and with whom it is connected .IBC use the single level public key cryptography and authenticity is the problem when security is concerned.IBC is further developed as IBE which is ID-based cryptography that uses the public key encryption method here users some of the unique information about the identity is used .next we have studied about Multi-authority ABE Scheme where the user is identified by a set of attributes and then some functions are used on those attributes to encrypt those attribute and decrypt those cipher text. In cipher text policy attribute based encryption, unlike traditional public key cryptosystem, different users may hold the same functional secret keys related with the same attribute set leading to additional difficulties in designing revocation mechanism. Ciphertext Policy Attribute based Encryption (CP-ABE), similar with role-based access control system, can be widely applied to realize access control. Managing user's identity ,access rights and providing adequate privacy and protection will be a great challenge because most providers are depending on different information systems to provide their services so in Identity and Access rights we haves studied one of the to hide or secure the identity and access rights of users from unauthorized user. Here we found application security and user access controls must compensate for the loss of network control and to strengthen risk assurance.

REFERENCES

1) Jianfeng Yang and Zhibin Chen, "Cloud Computing Research and Security Issues", Journal: 2010 International Conference on Computational Intelligence and Software Engineering Year: 2010 Pages: 1-3 Provider: IEEE Publisher.
2) Shuai Zhang, Shufen Zhang, Xuebin Chen and Xiuzhen Huo, "Cloud Computing Research and Development Trend," IEEE, Second International Conference on Future Networks, 2010.
3) R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.
4) X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.
5) R.Ranjith, S.Murugaanandam Department of IT, SRM University, Chennai, India " Privacy Preserving Authenticated Access Control with Decentralized Key Management in Clouds" 2014
6) "Management of Identity and Access in the Cloud" Sufyan T. Faraj, Sameeh Abdulghafour Jassim, Kashif Kifayat ,University of Anbar - College of Computer LJMU-School of Comp. & Math.Liverpool, UK J. of university of anbar for pure science : Vol.6:NO.2 : 2012
7) Boneh, D., and Franklin, M. K. Identity-based encryption from the weil pairing. In *CRYPTO* , pp. 213–229.
8) H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.
9) Sahai, A., and Waters, B. Fuzzy identity-based encryption. In *EUROCRYPT* (2005), pp. 457–473. Kungliga Tekniska Högskolan, "Exploring the limits of cloud computing," Master's Thesis, Stockholm, Sweden , October 4, 2010, pp.7-20.
10) K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, p. 419, 2012.[11]M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.

ISSN: 2278 – 1323

11) M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
12) A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
13) J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans.Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July2011.
14) M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABE Ciphertexts," Proc. USENIX Security Symp., 2011.
15) Token-Based Cloud Computing! A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.
16) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
17) W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Cloud Computing Security Workshop (CCSW), 2009.
18) S. Kamara and K. Lauter, "Cryptographic cloud storage," in *Financial Cryptography Workshops*, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

AUTHORS PROFILE

Miss. Pooja D. Bardiya Received the B.E in Information Technology and pursuing Masters in computer science and Information Technology from H.V.P.M College of engineering Amravati. Her research study Interest is in Data security and Information security. She has published papers that relates to the data security in cloud computing and she is doing research study secured and authenticated data access in cloud.

Prof.P.L.Ramteke is pursuing Ph.D in Mobile Computing he is Associate Professor and head of computer science and Information Technology in H.V.P.M College of Engineering Amravati. He has the Specialization in Mobile Computing, Software Engineering, Expert System and Design he has research experience of 3 years and published &papers in specialized topics above .He is member of various technical Institutes like ISTE, IAPT, and IAI.

ISSN: 2278 – 1323