Imparting Data in Cloud Storage using Key Revocation Process

R. Subbu Lakshmi[1] R. Nirmalan[2]
[1]P.G Scholar [2]Assistant Professor
[1,2]Department of Computer Science Engineering
[1,2]Sri Vidya College of Engineering and Technology

Abstract— Cloud computing is ideal for places where the data remain in a fixed environment, which are unavailable. Today imparting of data with security places is a major issue in cloud computing. For security issues key aggregate place a vital role to offer secured data transfer. Cloud storage is a storage of data online in cloud which is accessible from multiple and connected resources. Cloud storage can provide good accessibility and reliability, strong protection, disaster recovery, and lowest cost. This paper provides the various techniques and methodologies that can be used for security in revocation process and also new method proposed for data importing in cloud computing. This aggregate key can be sent to the others for decryption of cipher text set and remaining encrypted files outside the set are remains confidential. In order to protect the sensitive information in the cloud storage the key revocation is used.

Key words: cloud computing, data sharing, network security, and key revocation

I. INTRODUCTION

Cloud computing means provides computing over the internet and this word is basically inspired by the cloud. In this cloud computing, data is stored t remote location and available on demand and it allows clients to use applications without installation the file at any computer with internet facility. Many features are available in cloud computing such as resource pooling, on demand service, broad network access measured services and reduced cost of purchasing hardware and software. Usage of the software as a service and platform as a service and infrastructure as a service, user's data are stored in the cloud storage.

Cloud storage is used as a core technology of many online services for personal application. Cloud computing, all users are stored data on the cloud. So cloud user has to think about their data like, access control and authentication of the cloud. Cloud providers are maintaining the user's data in cloud environment. Cloud security and privacy of data are the major issues in cloud. Security and privacy re indeed interrelated because the security is provided without having privacy but the privacy is not maintained without security. Security is considered a key requirement for cloud computing consolidation as a robust and feasible multipurpose solution. Today various small and medium size companies moved towards cloud environment because bow they are capable to compete with the larger infrastructure companies by simply gaining fast access ton best business application at negligible cost.

Cloud security issues deals with all the challenges associated with securing an organizations core IT infrastructure at the network, host and application levels as well as the vulnerabilities and attacks related to the data security including data in transit, data at rest, processing of data including multitenancy, data lineage, data provenance, data lock in. The data in the cloud are subjected to attacks in either by hacker and provider. Analysis of attack in cloud computing such as network level attack, web application attack, language and malicious program injection based attack. The uses impart data in the cloud with a secure authentication and authorization. Imparting data poses several problems including privacy, data misuse. The data in cloud is laced in a share pool and breaches in data re major evolution to security. The imparting of data is necessary to share the sensitive information in a secured environment.

Cryptography is a technique applied for encryption and decryption. Crypotogrhy technique is referred as symmetric encryption and asymmetric encryption. Symmetric encryption is used in only one key for encryption and decryption. Asymmetric encryption is used in two keys for encryption is one key and decryption is one key. Cryptography access control is one of the most used techniques to securing data storage on entrusted servers where sensitive data has been encrypted before outsourcing and decryption keys are given only to authorize users without the decryption keys even the servers are not able to decrypts the data.

II. RELATED WORK

A. Symmetric-Key Encryption with Compact Key:

Benaloh et al. [2] presented an encryption scheme which is originally proposed for concisely transmitting large number of keys in broadcast scenario [3]. The construction is simple and we briefly review its key derivation process here for a concrete description of what are the desirable properties we want to achieve. The derivation of the key for a set of classes (which is a subset of all possible ciphertext classes) is as follows. A composite modulus is chosen where p and q are two large random primes. A master secret key is chosen at random. Each class is associated with a distinct prime. All these prime numbers can be put in the public system parameter. A constant-size key for set can be generated. For those who have been delegated the access rights for S' can be generated. However, it is designed for the symmetric-key setting instead. The content provider needs to get the corresponding secret keys to encrypt data, which is not suitable for many applications. Because method is used to generate a secret value rather than a pair of public/secret keys, it is unclear how to apply this idea for public-key encryption scheme. Finally, we note that there are schemes which try to reduce the key size for achieving authentication in symmetric-key encryption, e.g., [4]. However, sharing of decryption power is not a concern in these schemes.

B. IBE with Compact Key:

Identity-based encryption (IBE) (e.g., [5], [6], [7]) is a public-key encryption in which the public-key of a user can be set as an identity-string of the user (e.g., an email address, mobile number). There is a private key generator (PKG) in IBE which holds a master-secret key and issues a secret key to each user with respect to the user identity. The

content provider can take the public parameter and a user identity to encrypt a message. The recipient can decrypt this ciphertext by his secret key. Guo et al. [8], [9] tried to build IBE with key aggregation. In their schemes, key aggregation is constrained in the sense that all keys to be aggregated must come from different ―identity divisions‖. While there are an exponential number of identities and thus secret keys, only a polynomial number of them can be aggregated.[1] This significantly increases the costs of storing and transmitting ciphertexts, which is impractical in many situations such as shared cloud storage. As Another way to do this is to apply hash function to the string denoting the class, and keep hashing repeatedly until a prime is obtained as the output of the hash function.[1] we mentioned, our schemes feature constant ciphertext size, and their security holds in the standard model. In fuzzy IBE [10], one single compact secret key can decrypt ciphertexts encrypted under many identities which are close in a certain metric space, but not for an arbitrary set of identities and therefore it does not match with our idea of key aggregation.

C. Attribute-Based Encryption:

Attribute-based encryption (ABE) [11], [12] allows each ciphertext to be associated with an attribute, and the master-secret key holder can extract a secret key for a policy of these attributes so that a ciphertext can be decrypted by this key if its associated attribute conforms to the policy. For example, with the secret key for the policy $(1 \vee 3 \vee 6 \vee 8)$, one can decrypt ciphertext tagged with class 1, 3, 6 or 8. However, the major concern in ABE is collusion-resistance but not the compactness of secret keys. Indeed, the size of the key often increases linearly with the number of attributes it encompasses, or the ciphertext-size is not constant (e.g., [13]).

III. EXISTING SYSTEM

In key-aggregate cryptosystem (KAC), users encrypt a message not only under a public-key, but also under an identifier of ciphertext called class. That means the ciphertexts are further categorized into different classes. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for different classes. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.[1] With our example, Alice can send Bob a single aggregate key through a secure e-mail. Bob can download the encrypted photos from Alice's Box.com space and then use this aggregate key to decrypt these encrypted data. The sizes of ciphertext, public-key, master-secret key and aggregate key in KAC schemes are all of constant size. The public system parameter has size linear in the number of ciphertext classes, but only a small part of it is needed each time and it can be fetched on demand from large (but non-confidential) cloud storage.

IV. PROPOSED SYSTEM

In this project, Sender can send the collection of data to the receiver. If the sender unfortunately sends his personal data to receiver, and the sender wants to delete the key and sender can send the new key to the receiver. This process is called as the key revocation process. To provide secure data sharing in cloud storage using Key aggregation. In order to protect the sensitive information in the cloud storage the key revocation is used.

A. Architecture of the Proposed System:

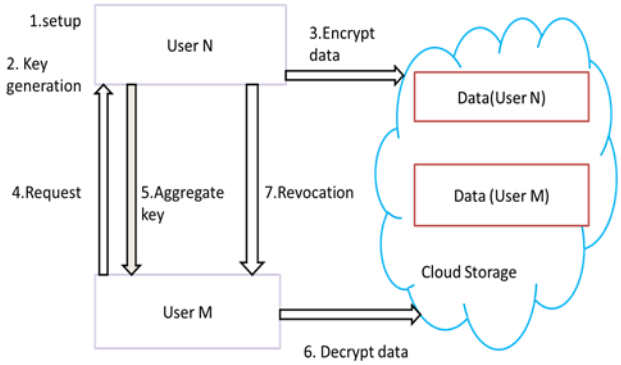


Fig. 3.1: Proposed System Architecture

B. Description of Proposed System:

In this project, we have to first create repository and access method to use sender and receiver and then collect the identity and name and automatically generate the IP address. We must also extract the data and these data form such as pdf, ppt and image. Next generate the key using only authorized user.Data stored in the cloud using encrypted forms. These encryption algorithm using blowfish and generate the master key and secret key. These two keys are XOR operation and produce the aggregate key. After the response from the data owner, the receivers get the aggregate key to access the data in the cloud. Upon the usage of data the aggregate key is revocated to prevent the user from accessing the data when sensitive data is placed.

V. MODULES

A. Key Generation:

In cryptographic environment key generation is using lot of algorithm, such as RSA, Elliptical curve cryptography & Diffie Hellman key exchange.

B. RSA Algorithm:

RSA is makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number. The blocks must be less than (or) equal to $\log_2(n)$, block size is i bits, where $2^i<n<2^{i+1}$

1) Steps:

1) Select p, q p!=q
2) Calculate n= p*q
   $\Phi(n)= (p-1)(q-1)$
3) Select integer e, $\gcd(\phi(n),e)\equiv 1$, $1<e<\phi(n)$
4) Calculate d, $d\equiv e^{-1} (\mod (\phi(n)))$
5) Public key PU = {e, n} e=encryption
6) Private key PR = {d, n} d=decryption

C. Elliptical Curve Cryptography:

Private Key is considering by the curve. Private Key is considering by random number. The public key is generated by multiplying private key with generator by G. key generation is n important port. An algorithm should generate both public key and private key. The sender will encrypt the

message with the receiver public key and receiver will decrypt with its private key.

Select a number; d in range of n we use the public key such as,

- Q=d*p
- Q=public key
- P=point on curve
- D=private key

D. Diffie Hellman Key Exchange:

Diffie and martin Hellman introduced key exchange protocol with the use of the discrete logarithm problem. In this protocol sender and receiver will setup a secret key to their symmetric key system, using an insecure channel. To setup a key Alice chooses a random integer a€[1;n] computes g^a, similarly bob computes g^b for random b€ [1;n] and sends it to Alice. The secret is gab, which Alice computes by computing $(g^b)^a$ and bob by computing $(g^a)^b$.

- Input= G is an Abelian group, g€G, in is prime multiplicative order
- Output= A secret S€G , which will be shared by both the sides.

1) Steps:

1) Sender generates random d_A€{2……m-1}
2) Compute $e_A=g_A^d$
3) Sender sends e_A to receiver
4) Receiver generate random d_B€{2……m-1}
5) Compute $e_B=g_B^d$
6) Receiver sends e_B to Sender
7) Sender calculate S= $(e_B)_A^d=g_A^d d_B$
8) Receiver calculate S= $(e_A)_B^d=g_A^d d_B$

Cipher class consisting of data owner's id and message and the master key (or) public key of the data owner attributes. Using master key, public key is generated and secret key is generated by doing the logical XOR operation. Ciphering algorithm are applied using the secret key, thus secured secret key is generated by key aggregate cryptosystem. The key generation algorithm run by public key takes as input is master key(MK), identity(ID), revocation list (RL), time list (TL).the algorithm is aborted, if ID€RL otherwise it sends the private key SK_{ID}= { IK[ID], $TK[ID]_{Ti}$} to the user. Where IK [ID] is the identity component or private key, TK [ID] is its time component for current time period T_i. Data owner establishes the public system parameters and generates a public key and master key pairs using key generation algorithm. Cipher text policy attribute based encryption using key generation in this case generate the public key and master key using the diffie Hellman key exchange algorithm.

VI. KEY AGGREGATION

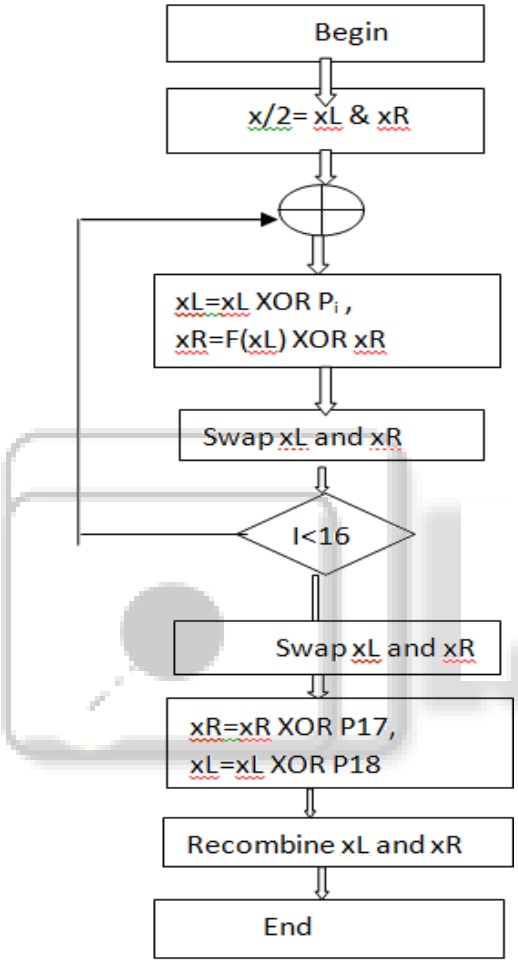
Aggregate key is used for the secure data sharing over the distributed data sharing in cloud environment. Aggregate key consist of various derivation of identity and attribute based classes of respective data owner in the cloud. Combination of several key acts as a single key is called key aggregation. To avoid active attack, key aggregation process is performed. An Active attack is an attack characterized by the attacker attempting to break into the system. The intruder will introduce data into the system as well as potentially change data within the system. Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into different categories. An active attack attempts to alter system resources or affect their operation. Types of an active attack such as modification attack, reputation attack, denial of service attack, backdoor attack, man in middle attack, reply attack. Aggregation key is the process of pairing up the attribute information and using master key and logical derivations of the data owner attributes. Aggregate key is considered as secret key for data security for the data being outsourced in the cloud. Key aggregation cryptosystem is unique key generation scheme for secure and robust cloud data security mechanism. In which produce effective constant size private key by means of derivation of different cipher text classes. It differs from the normal cryptography techniques by generating the keys from the various attributes of data owner.

Aggregation key is used to sharing the data between one user to another user. The key aggregation property is especially useful when we expect the delegation to be efficient and flexible. Key aggregation is enable a content provider to share her data in a confidential and selective way, with a fixed and small cipher text expansion, by distributing to each authorized user a single and small aggregate key. Alice wants to share the data on the server. First to get the username, password and to execute key generation. The key generation phase is providing by public key and master key pair. In this public and master key pair is secret by Alice. Alice encrypts the data using public key and these data are uploaded to the server. Alice is willing to share a data to bob. Alice can compute the aggregate key for bob, it's performed by master key, and these aggregate key is sent to bob via email and these aggregation key is using to downloaded the data and decrypt the data. Exact is executed by the data owner for delegating the decrypting power for a certain set of cipher text classes to a delegate. In this example input is master key and data and output is aggregate key. It's the primary key having more than one column. Key aggregation is group of public key and private key used for transmission of data. The combination of public and private key is known as key aggregation. Key is nothing but composite or concatenated key. Example different books may have identical title, authors. In this case we can take title, author, and publication date as the aggregate key which acts as primary key. Map reduce function is also used in key aggregation. Advantage of key aggregation is such s secure key cryptographic derivation, higher data security, supports data integrity process, and also easy to manage the all keys. For security issues key aggregation places a vital role to offer secured data transfer. Key aggregation cryptosystem is a unique key generation scheme for secure and robust cloud data security mechanism, in which produce effective constant size private key by means of derivation of different cipher text classes. It differs from the normal cryptography techniques by generating the keys from the various attributes of data owner

VII. BLOWFISH ALGORITHM

Blowfish has a 64 bits block size and a variable key length from 32 bits up to 448 bits. And it's a variable length key block cipher. Blowfish is a symmetric block .cipher that can be used as a drop-in replacement for data encryption algorithm DES) and international data encryption algorithm

(IDEA). Much faster than DES and IDEA. There are two parts to this algorithm such as key expansion, data encryption. Key expansion breaks the original key into a set of sub keys. There is a P-array and four 32 bit S-boxes. The P-array contains 18 32-bits sub keys, while each S-box contains 256 entries. Data encryption contains 64 bit input is denoted with an x, while the P-array is denoted with a P_i (where I is iteration). In this modification of F function is using multithreading concept and its performed by parallel execution. Time taken of complete 16 gate operation is equal to time taken of complete 32 XOR operations. Since all the operations are running in parallel environment.



Data encryption occurs via 16 round festial network. Each round consists of key depenednt permuttion, and a key nd data dependent substitutions. All operations are XORs and addtion on 32 bit words. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

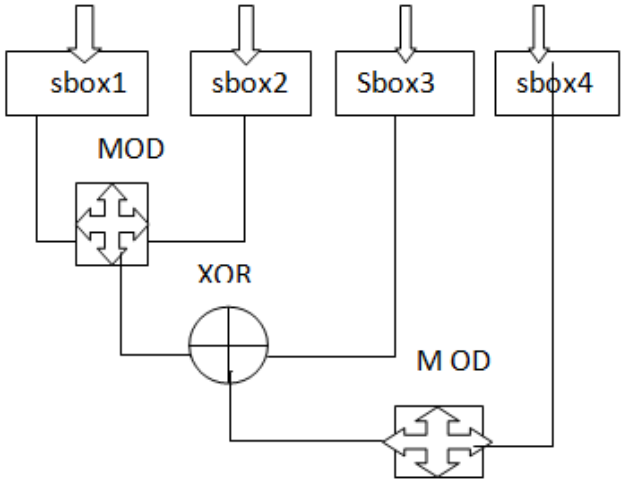
VIII. ENCRYPTION

- Blowfish has 16 rounds.
- The input is a 64-bit data element, x.
- Divide x into two 32-bit halves: xL, xR.
- Then, for i = 1 to 16:
- xL = xL XOR Pi
- xR = F(xL) XOR xR
- Swap xL and xR

After the sixteenth round, swap xL and xR again to undo the last swap.

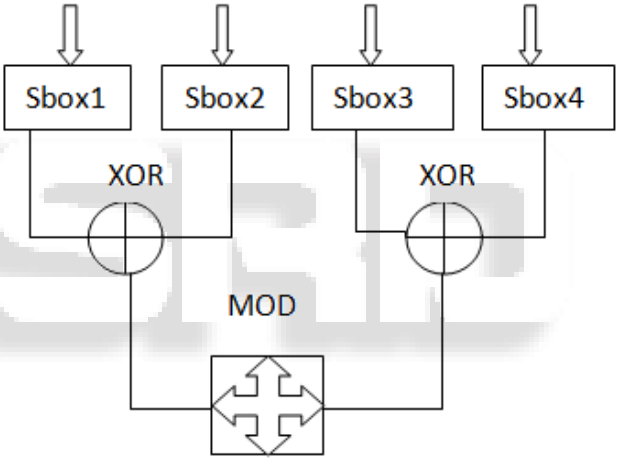
A. F Funtion:

$F(X)=((S_1+S_2 \bmod 2^{32})XOR\ S_3)+S_4 \bmod 2^{32}$



B. Modification of F Function:

$F(X) = ((S_1\ XOR\ S_2 \bmod 2^{32})+(S_3\ XOR\ S_4 \bmod 2^{32}))$



In this modification of F function is using multithreading concept and its performed by parallel execution. Time taken of complete 16 gate operation is equal to time taken of complete 32 XOR operations. Since all the operations are running in parallel environment. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order.

IX. KEY REVOCATION PROCESS

Revocation is act of recall or annulment. Revocation list is performed by some operation in cryptosystem such as public key infrastructure and certificate revocation list. In this certificate revocation list is a list o certificates that have been revoked. Main use of revocation is unspecified, key compromise, certificate authority compromise, affiliation changed, superseded, cessation of operation, certificate hold, remove from certificate revocation list, privilege withdrawn. Main function of revocation is performed by identity based encryption system and using key management. In this identity based encryption can support more entities than public key infrastructure while applied to the complicated system such as the cloud computing. Authentication system can be deployed in different ways such as centralized

manner and distributed manner. Revocation mechanisms such as certificate revocation list, certificate revocation status, online certificate status protocol, certificate revocation tree, security mediator. The Key revocation process is needed when sensitive data is placed on the cloud storage. Data retrieved process not only consist o retrieved of encrypted files from the cloud server and decrypted using respected private keys. But the data are provided to the users upon the authentication of the hierarchical access control of cloud system architecture. Key revocation refers to the task of securely removing compromised keys. Data (or) keys are revocated in the cloud frequently depending upon the kinds of data owner's identity and the data to be stored on the cloud. Revocation event occurs the data owner redefines the master key component and public key component corresponding to variable attribute and then re encrypt the data using the new public key component. Key revocation, which describes, how to remove secrets that may have been compromised. Revocation mechanisms are known in identity based encryption such as renew their private key periodically and senders use the receivers identities concatenated with current period. In this mechanism would result in n overhead load in public key generator. Revocation scheme is based on one way accumulator has both the one way and quasi commutative property, based on strong RSA assumption. Modified cipher policy attribute based encryption to setup a fine grained access control method in which user revocation is achieved based on the theory of Shamir's secret sharing. User revocation is challenging issues in these attribute based encryption, based solution since it would inevitably require data reencryption and may need user secret key updates. To reduce the cost for secret key updates, the cloud servers perform a lazy update, which means the users' secret keys are only updated when they setup a legal request. To provide a seamless integration between the revocation and tracing so that the tracing mechanisms does not require any change to the revocation algorithm. Identity based encryption using user revocation. The revocation algorithm run by public key generator takes as input is such as a revocation list, a time list and set of identities to be revoked and its output is such as update revocation list and time list.

X. CONCLUSION

Overall an aggregate key Cryptosystem is generated which produce effective constant size private key by means of derivations of different cipher text classes. Proposed approach provides secure and efficient cryptographic scheme in which an effective derivation of secret key generation and key management for the outsourced Cloud data. Using blowfish algorithm to increase security. This algorithm used for user friendly process and manner. The enhanced encryption algorithm can be used to encrypt the data which is stored in cloud. An acknowledgement can send to the user holding the aggregate key about the key revocation time.

REFERENCE

[1] Cheng-Kang Chu, Sherman S.M.Chow, Wen-Guey Tzeng, jianying Zhou,"key aggregate for Scalable Data Sharing in Cloud storage ", vol 1045-92 2013.

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage," IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013.

[3] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE-Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security - ACNS2012, ser. LNCS, vol. 7341. Springer, 2013, pp. 526–543.

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[5] Jin Li, Jingwei Li, Xiaoeng,Chunfu Jia and Wenjing Lou," Identity based Encryption with outsourced Revocation in cloud computing", vol0018,2013

[6] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser.LNCS, vol. 6805. Springer, 2013, pp. 442–464.

[7] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2013;.

[8] T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu, "Identity Based Encryption Resilient to Continual Auxiliary Leakage," in Proceedings of Advances in Cryptology - EUROCRYPT '12, ser. LNCS, vol. 7237, 2012, pp. 117–134.

[9] Jashnapreet pal kaur, rajbhupinder kaur, "security issues and use of cryptography in cloud computing", in international journal of advanced research in computer science engineering-volume 4, issue 7, july 2012.

[10] Nagamalleswara rao.dasari, vuda sreenivasaro, "performance of multi-server authentication and key agreement with user protection in network security", volume 02, No. 05,2010, 1705-1712.

[11] Neha tirthani, Ganesan R,"Data security in cloud architecture based on Diffie Hellman and Elliptical Curve Cryptography", volume 8, 2010,

[12] L.Arockiam, S. Monikandan,"Data Security and Privacy in cloud storage using hybrid symmentric encryption algorithm" volume 2, issues 8, 2010;

[13] H. K. Maji, M. Prabhakaran, and M. Rosulek, ―Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,‖ IACR Cryptology ePrint Archive, 2008.

[14] D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," in Proceedings of Advances in Cryptology - CRYPTO '01, ser. LNCS. Springer, 2001, pp. 41–62.

[15] Rashmi Nigoti, Manoj Jhuria Dr.Shailendra Singh," A survey of Cryptography algorithm for cloud computing", IJETCAS 13-123 2001.

