A Study on the Security Issues , Algorithms and Schemes towards a more secure Cloud Storage

Shanthi D.L [1], Sahana .P [2], Abishek .P [3], Shilpa A.S[4] , Juhi Kumari [5]

[1] Assistant Professor, Dept. of ISE, BMS Institute of Technology, Bangalore .

[2] ,[3] ,[4] ,[5] Student, Department of ISE, BMS Institute of Technology, Bangalore .

Abstract— Cloud computing provides access to system resources and information using remote servers connected via the internet. Cloud provides shared resources like networks, processing power and data storage space. Due to recent advancements in digitalization and computing power, huge volumes of data are generated by enterprises. Thus cloud provides a cheaper and efficient solution to tackle this problem.

Since security in cloud is provided by a third party vendor it becomes important to confront with issues like trust, confidentiality and integrity. Various schemes and algorithms have been established to ensure secure cloud storage and sharing. A study of the issues regarding cloud storage is made .Traditional security algorithms are classified as symmetric and asymmetric are studied and compared .Various schemes proposed that pave the way towards a more secure cloud storage and sharing are studied and analyzed .This paves the way to study the evolution of security algorithms for cloud security from its roots via conventional schemes to its modern day interpretations .A conclusion is then drawn from the study.

Keywords — security issues, cloud security algorithms, symmetric algorithms ,asymmetric algorithms, attribute based encryption (ABE), homomorphic encryption, identity-based encryption (IBE) with compact key, key aggregate cryptosystem

IJSER

I. INTRODUCTION

A cluster of servers and datacenters located at geographically diverse areas that provide on demand services using internet is known as cloud. The components of cloud include distributed servers, clients and data centers. Clients are devices that the end users use as an interface to manage their data on cloud that include PDAs, personal computers, mobile phones, tablets etc. The datacenter is a cluster of servers where the services to which the clients subscribe are hosted. The distributed servers provide location transparency and on demand services in cloud. The five key characteristics of cloud computing are namely on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity and scalability.

Cloud eliminates the need to worry about the maintenance of hardware, software and storage space as these services are provided by a third party service provider. The cloud service provider charges the user based on the usage of the services, making cloud a cheaper technology to use. Other important benefits of cloud include multi-tenancy (allowing resources to be shared by many users), device independence, scalability and flexibility. Thus the above benefits add impetus to the fast growth of cloud computing. When private information is stored on the cloud then security becomes a huge matter of importance as the data on the cloud is not directly managed by the user [1]. The data on cloud is secure if the issues of privacy, confidentiality, integrity, availability and trust are taken care. The major examples of cloud services include social networking sites like facebook, email services provided by gmail and other business applications. As cloud computing is a new computing model there is lot of uncertainty about how security at all levels like network, host, application and data level can be achieved. Security concerns with respect to data, access, data classification, service level agreement and security breach are also considered. The security risks due to viruses, Trojans, spoofing, root kits should not be ignored. The conventional security mechanisms are no longer enough for cloud in their current form.

II. PROBLEM FORMULATION

The cloud service users put a large amount of data into cloud storage and transfer the burden of storage and computation on to the cloud. On the other hand it is important for the users to ensure that their data is stored safely and privacy is preserved. Hence main aim of this paper is to identify and organize the most relevant security issues and solutions in the present context pertaining to the cloud. Since security in cloud is of utmost concern for many organizations,we make a detailed study on a few cloud security algorithms like Data encryption Standard (DES), Advance encryption algorithm (AES), Triple-DES, Blowfish Algorithm, Idea, RSA, Diffie- Hellman Key

Exchange in section V. We then present a comparison of these traditional algorithms in section VI. Later we introduce schemes towards effective encryption and conclude with an analysis on the algorithms and study on the schemes in section VII. The concepts and keywords related to this topic include security issues, cloud security algoritms,Symmetric algorithms,Assymetric algorithms, Attribute Based Encryption (ABE), Homomorphic Encryption, Identity-Based Encryption (IBE) with Compact Key, Key Aggregate Cryptosystem .

III. RELATED WORK

The main challenges faced are in cloud are in the area of security.Lot of work pertaining to security issues have been carried out. Security issues are broadly classified as threats and vulnerabilities. Some research papers classify them as separate entities and study the effect of their inter-relationship on cloud security.These issues may seem generic and may apply to any new technology.But it they are very vital in the cloud scenario.To address these issues many researchers propose the data placed in the cloud should be encrypted. AES based file encryption system is used in some of these models. In this encryption scheme both the encryption key and the encrypted file are maintained on the same server. A malicious attack in the server may leak all the information to the hacker. For best security ensuring process , the Recently models based on key aggregation ,identity based encryption ,homomorphic encryption are reasearched that provide more privacy and security compared to the traditional models.

IV. ISSUES IN CLOUD STORAGE

Security in cloud is related to issues like external data storage, dependency on the internet, loss of control, lack of trust and multi-tenancy. Many cloud service users are apprehensive about the vulnerabilities in cloud like data related vulnerabilities, insecure interfaces, vulnerabilities in virtual machine and networks etc. Cloud providers are constantly trying to mitigate these drawbacks by providing substantial resources. Some of the privacy and security issues related to cloud storage include:

i) Privacy

With an increase in digitalization privacy issues are becoming more critical in today's computing world. User's data may be spread even various geographical locations. Based on the tasks submitted by users from different locations hackers have the ability to predict the future tasks. Some of the major privacy issues include trust issues that concerns with unauthorized usage of Private Information. Uncertainty deals with whether data has been properly destroyed by the data owner and on how the privacy breaches have occurred. The common concerns related to privacy in cloud for users include:

1. How confidential is an organization's data on cloud?
2. What measures should be employed to preserve the privacy of the users?
3. Measures ensuring access control and identity management.

ii) Trust

Trust in cloud computing is measured in terms of the quality attributes like integrity, strength, ability and reliability. Trust issue in cloud is as important as security and privacy because trust is important for the user to share his data on cloud. Still cloud has failed to provide trust between customer and provider. Weak trust relationship between the service provider and user can cause many problems during deployment of cloud services. One such example came to light when amazon' elastic compute cloud service crashed during system upgrade. The concern with respect to trust is trust worthiness of the interfaces and API provided by the service providers.

iii) Identification & Authorization

The types of cloud which is private, public or hybrid, transmission model, access requirements and security of the clients determines the performance of cloud computing processing. The issue of identification and authorization is solved using passwords and usernames so that the correct user gets access to his content on cloud. Authorization is maintained by the service provider .Researchers are in constant quest for better authorization techniques because it is a vital information security requirement in cloud. Concerns regarding identity management, encrypted data communication are to be handled under this issue.

iv) Confidentiality

Confidentiality means that the data owner's data and tasks are to be kept in secret from both the cloud provider and other users of the cloud service. Thus prevents the disclosure of private information to third party service providers. Providing privacy to clients' data and securing their information deals with handling data security issues at different distinctive layers of cloud. Concerns with respect to confidentiality include:

1. The compliance of cloud providers with regulation.
2. As services in cloud are housed on a common software stack, the treats and vulnerabilities of common software stack must be tackled.

V. CONVENTIONAL SECURITY ALGORITHMS FOR CLOUD

Data on the cloud can be secured by posting encrypted information on to the cloud. There are many encryption algorithms proposed to secure the data on cloud, which can be classified as Symmetric and Asymmetric algorithms. The symmetric algorithms include DES, AES, Triple DES, Blowfish. The asymmetric algorithms include RSA,DSA , Diffie Hellman. DES was developed in early 1970s.Whereas the Blowfish algorithm was developed by Bruce Schneier, in the year 1993. AES was developed by NIST in the year 2001.All of these algorithms use symmetric key encryption, where a single key is used for encryption/decryption of tcipher

text. On the contrary, asymmetric algorithms use separate keys for encryption and decryption of the cipher text.

i) ASYMMETRIC ALGORITHMS

i. a) RSA :

The RSA algorithm is named after its founders Ranold Fivest, Adi Shamir and Leonard Adleman. This algorithm falls into the asymmetric category of algorithms. The digital signatures of many software services and product use this algorithm. Working of RSA is based on the multiplication of two relatively large prime numbers. Private and public key are generated by taking the modulus of number generated by multiplication. A variable size key and encryption block are used in this algorithm. Each of the prime numbers chosen may be 100 or more digits in length. As the prime factors of the large number are difficult to determine it becomes hard for the hackers to determine the private and public keys, thus making RSA a more secure algorithm.

ALGORITHM:

1. Consider two large prime numbers *r* and *s*.
2. Calculate $n = r * s$.
3. Calculate $z = (r – 1) *(s – 1)$.
4. Choose‘ *t* ’ such that t is relatively prime to *z* and less than *z* .
5. Determine ‘*d*‘ such that $(d * t) \% \varphi(n) = 1$ and d < *z*.
6. The Public key = {t, n}, Private Key = {d, n} and Cipher text c = *message s mod n* ,Plain text p = *cipher text d mod n.*

i . b) Diffie-Hellman

Diffie Hellman key exchange algorithm was proposed by Whitfield Diffie and Martin Hellman in the year 1976. This algorithm provides a way to safely exchange keys over a public medium. This algorithm falls into the category of public-key cryptography. Following are the steps for Diffie Hellman algorithm:

1. Sender and receiver select a number each which is known to both of them. Assume the selected number by the sender to be *S* and the number selected by receiver to be *R*.
2. Sender and receiver calculate the secret key using the above two numbers P_a.
3. Ps is calculated as $P_s=g^{sr}$ mod k. where g=|k| and k is a large prime number less than k.
4. P_s and P_r are calculated
5. The sender and receiver exchange values with each other to check if the correspond to each other
6. If the above step is true then communication begins.

i . c) EI Gamel

The ElGamal algorithm is an asymmetric key encryption algorithm discovered in the year 1984. This algorithm is used to secure softwares like GNU Privacy Guard and in many other cryptosystems. This encryption technique can be defined over any cyclic group. Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms. A PKC system similar to Diffie-Hellman is used for key exchange.

ii) SYMMETRIC ALGORITHMS

ii . a) DES

Data encryption standard algorithm was a commonly used encryption technique that was found in the year 1974 by IBM. This encryption technique houses complex set of rules that are used to provide efficient hardware implementations. A block cipher is of 64 bits and a key of 56 bits is used [2]. The major shortcoming of the DES technique is that the key used very small, hence making it more vulnerable to security breaches. Two important variants of DES are Triple-DES (3DES) and DESX.3DES uses three 56-bit keys and makes three encryption/decryption passes over the cipher block. DESX adds an extra 64 key bits to the plaintext before the encryption process. Thus this variant increases the key length to 120 bits making it more secure.

ii . b) BLOWFISH

Blowfish Algorithm is a symmetric key algorithm which was developed in 1993 by Bruce Schneier. Its working is almost similar to DES. In DES algorithm key size is small and can be decrypted easily but in contrary Blowfish algorithm has large key size that can vary from 32 to 448 bits. Blowfish consists of 16 rounds like DES. Blowfish algorithm can encrypt data having sizes in multiples of eight and if the size of the message is not a multiple of eight then bits are padded. The algorithm divides 64 bits of plain text into two parts of size 32 bits. One part is taken as the left part of message and the other as the right part of message.

ALGORITHM :

1. Divide the message *M* into two 32-bit halves: *xL*, and *xR*
2. Repeat the following steps for 16 times
   Compute xL= xL XOR Pi
   Compute xR = F(xL) XOR xR
   Swap xL and xR
3. Undo the last swap
4. xR = xR XOR P17
5. xL = xL XOR P18
6. Recombine xL and xR .

ii . c) AES

Advanced Encryption Standard (AES) algorithm uses a symmetric key encryption technique and was found in the year 2001. This algorithm uses variable block length and key length. The key size may be 128, 192 or 256 bits in length.
In AES, different size of key is used i.e. 128, 192 or 256 bits.

IJSER

Algorithm	DES	Blowfish	RC5	Triple DES	AES
Block size	64	64	32,64,128	64	32,64,128
Key length	56	32-448	MAX2040	112,168	128,192,256
Security	Inadequate	Secure	Secure	Secure	Secure
Speed	Very slow	Fast	Slow	Slow	Very fast
Scalability	Scalable due to the block size	Scalable	Scalable	Scalable	Scalable

The key size is selected based on the number of cycles the key is used, example: 10 cycles require a key length of 128-bit, whereas 12 cycles use a key length of 192 bit. AES uses small 4x4 matrixes having the steps of key expansion, initial and final round. Initial round consist of Add Round Key, Sub Bytes, Shift Rows, Mix Columns, Add Round Key and final round. AES functions equally efficiently both on hardware and software devices.

ALGORITHM:
Cipher(byte[ ] input, byte[ ] output)
Begin
byte[4,4] State;
copy input[ ] into State[ ] AddRoundKey
For round = 1 to round < Nr-1
SubBytes
ShiftRows
MixColumns
AddRoundKey
EndFor
SubBytes
ShiftRows
AddRoundKey
copy State[ ] to output[ ]
End

ii . d) RC5

The RC5 was developed in 1994. The key length is taken as MAX 2040 bit with a block size of 32, 64 or 128. The important advantage of this algorithm is that it is secure but the speed is slow.

ALGORITHM:
Compute A = A + S[0];
Compute B = B + S[1];
For i = 1 to r do
A = ((A Xor B) <<< B) + S[2 * i]
B = ((B Xor A) <<< A) + S[2 * i + 1]
EndFor

VI. COMPARISON

A detailed comparison between symmetric and asymmetric algorithms is presented in this section as depicted in *Table I.* In addition to the above comparison details the important difference between symmetric and asymmetric algorithms is that symmetric algorithms like DES use the same key for encryption and decryption whereas asymmetric algorithms like RSA use different keys for encryption and decryption. Algorithms like DES use message authentication whereas algorithms like RSA use robust authentication implementation.

VII. RECENT SCHEMES TOWARDS EFFECTIVE ENCRYPTION

Over the many years various new schemes and cryptosystems have been proposed .The Attribute Based Encryption [2] ,[3] Technique allows an attribute to be associated with each ciphertext which could be decrypted only by a conforming key .Identity Based Encryption [4] ,[5] ,[6] allowed an Identity string to be associated with the public-key of every user .Homomorphic encryption schemes allowed for operations to be carried out on ciphertexts reflecting the result of the operation if carried out on plain texts itself .The Key Aggregate Cryptosystem [7] enabled decryption of a number of ciphertexts using a single key that was compact .These schemes have paved the way to a more efficient and secure storage and sharing in cloud as discussed further .These schemes are more efficient relative to the conventional schemes in the sense that they provide some gain like increased security or decreased costs etc .

i) <u>Attribute Based Encryption (ABE) :</u>

Attribute Based Encryption (ABE) ,a form of public-key encryption ,is a scheme of encryption where both the secret key of a user and the ciphertext are dependant on some attributes .The attributes specified can be any key property of that individual such as his native country ,type of subscription he possesses etc .In this type of scheme for encryption ,decryption of the ciphertext is achieved only if the set of attributes of the user key matches attributes of the ciphertext . The concept of attribute-based encryption was first proposed in a landmark work by Amit Sahai and Brent Waters .This scheme possesses good collusion-resistance capabilities . However it posses two challenges non-efficiency and non-existence of attribute revocation mechanism .This scheme has two major sub-groups Ciphertext-policy ABE (CP-ABE) and Key-policy ABE (KP-ABE) .ABE is also the generalisation of another encryption scheme known as Identity Based Encryption(IBE). ID-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based

IJSER

cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address).

Ciphertext-**policy Attribute Based Encryption (CP-ABE) :**

In Ciphertext-Policy ABE mechanism ,access strategy is in control of the encryptor .The complexity of the design of the system public key increases with increasing complexity in the access strategy . This scheme can be considered as a generalization of Identity Based Encryption but proves to be more flexible . There is a single public key and a master private key that is used to produce private keys . The private keys are associated with sets of attributes or labels, and when encryption is done, we encrypt to an access policy which specifies which keys will be able to decrypt the data allowing complex rules specifying which private keys can decrypt which ciphertexts .

Key-policy Attribute Based Encryption (KP-ABE) :

Key-Policy ABE is an important class of Attribute Based Encrytpion where the ciphertexts have sets of attributes associated with them and private keys depend on the access structures controlling the ciphertexts a user is able to decrypt . This scheme has vital applications in the field of data sharing on public cloud storage. But the major disadvantage of this method is that the size of the cipher text increases proportionaly as the number of attributes inside the cipher text increases.

ii) Homomorphic Encryption:

This type of encryption method permits computations to be carried out on ciphertext. The computations on the ciphertext give an encrypted output which on decryption matches the result of the operations performed on the plain text. This encryption scheme produces a modifiable design, thus providing integrity and confidentiality of the data to be sent. Homomorphic encryption schemes are classified into partially homomorphic and fully homomorphic scheme. Homomorphism is understood taking the RSA algorithm as an example,

If the public key in RSA is modulus *'m'* and exponent *'e'*, then the encryption of a message *'x'* is given by *'$\epsilon(x) = x^e \bmod m$'*. The homomorphic property is then

Eq1. $\epsilon(x_1) . \epsilon(x_2) = x_1^e x_2^e \bmod m = (x_1 x_2)^e \bmod m = \epsilon(x_1 . x_2 \bmod m)$.

Partially-Homomorphic Encryption Schemes :

A cryptosystem that shows either additive or multiplicative but not both at the same time is called partially homomorphic.Thus ,this subset of homomorphic schemes allows only limited computational capabilities ,i.e.,operations that can be performed on the ciphertext are limited .These schemes allow only specific computations to be carried out onto the ciphertext . Processing time and implementation complexity are key advantages of this subset over Fully Homomorphic Encryption Schemes. There exist many cryptosystems that are partially homomorphic like unpadded RSA system and ElGamal system that exhibit multiplicative homomorphism ,and the Pailler system that exhibits additive homomorphism .

Fully-Homomorphic Encryption schemes :

A cryptosystem is considered fully homomorphic if it exhibits both additive and multiplicative homomorphism .Thus ,fully homomorphic encryption schemes allow great flexibility in operations that can be carried out onto the cipher text .They posses great computational capabilities and allow creation of generic constructs for computations . As this technique need not decrypt its input, it can be used in an untrusted environment without letting out it's input and internal state. The first such construct was proposed by Craig Gentry in 2009 .The proposed model was a lattice-based cryptosystem that relies on a complex mesh of ideal lattices for representing the keys and the cipher text .The next system was proposed in 2010 built with Gentry's construction as a foundation and did not require ideal lattices . Many new schemes came into existence in the year 2011-2012, thus paving a way for more efficient and fully homomorphic cryptosystems. These include:

- The Brakerski-Gentry-Vaikuntanathan cryptosystem (BGV), building on techniques of Brakerski-Vaikuntanathan .
- Brakerski's scale-invariant cryptosystem.
- The NTRU-based cryptosystem due to Lopez-Alt, Tromer, and Vaikuntanathan (LTV).
- The Gentry-Sahai-Waters cryptosystem (GSW) .

iii) Identity-Based Encryption (IBE) with Compact Key :

Identity-Based Encryption as mentioned is a specific scenario of ABE .It is a public-key encryption scheme where the public-key can be set as the identity-string of the user (e.g., an email address, mobile number ,etc) .The Private Key Generator (PKG) holds a master secret key specific to each user with respect to his/her identity .The encryption is done with the help of the public parameter and user identity and the recipient decrypts the message using the secret key . Guo et al [8] ,[9] made first advances to building an IBE scheme with key aggregation with the constraint that all keys to be aggregated must belong to different " identity divisions" .Thus ,only polynomial number of keys could be aggregated whereas

IJSER

number of identities and hence secret keys are exponential .An alternative approach to this scheme involved using a hash function to the string denoting the class . In fuzzy IBE , one single compact secret key can decrypt cipher texts encrypted under many identities which are close in a certain metric space, but not for an arbitrary set of identities .

iv) Key Aggregate Cryptosystem :

The encryption of messages in the Key Aggregate Cryptosystem (KAC) is done not only under a particular public key but also in accordance with an identifier of the cipher-text called class .A cipher text class is an arbitrary integer defining a classification as made by the data owner under which the plain text is to be encrypted .Thus ,the cipher texts are categorized into different classes .The key owner owns a master-secret called master-secret key ,which can be used to extract secret keys for different classes [7] .The key that is extracted can be an aggregate key which combines the power of many secret keys allowing the decryption of more than one cipher text with the same aggregate key . The sizes of cipher text ,public-key ,master-secret key ,and aggregate key in the KAC scheme are all of constant size .This provides great time and security advantages over the one key per request for file and one key for all files schemes respectively .A general framework for KAC [7] for scalable data sharing in cloud storage proposed by Cheng-Kang Chu ,Sherman S.M. Chow ,Wen-Guey Tzeng , Jianying Zhou, and Robert H. Deng is as follows ,

(a) Setup Phase: The data owner executes this phase to register his/her account on an un-trusted server. This step also deals with deciding the number of cipher-text classes .
(b) Key Generation Phase: Executed by the data owner to randomly generate a public / master–secret key pair .
(c) Encrypt Phase: Executed by any user in order to encrypt the data .This is done using public key ,index (denoting the cipher-text class), and the message and delivers the cipher-text.
(d) Extract Phase: This phase is executed by the data owner for delegating the decrypting power for a certain set of cipher-text classes to a delegate .It uses the master-secret key and set of indices of the cipher-text classes and outputs the aggregate key.
(e) Decrypt Phase: This phase is executed by a delegate who received an aggregate key generated during extraction phase. This phase results in decrypted data to be presented to the delegate.

A limitation of the above scheme is the predefined bound of maximum number of cipher text classes .In cloud storage environment, this parameter grows rapidly and thus ,a scheme that is independent of number of cipher text classes is an area for future work .

CONCLUSION

The major security issues with respect to cloud include privacy, trust, data portability and conversion, integrity, authentication. But the most important of them is security and how cloud providers are assured of it. Cloud computing has several customers from various backgrounds like ordinary users, academia, and enterprises .If cloud clients are academia ,performance along with security issues are to be taken into account. From an enterprise's point of view security is of higher priority compared to high performance. Security is thus viewed from different point of view by different users based on their requirements. We thus analyze traditional security algorithms in cloud by dividing them into two categories namely symmetric and asymmetric .These algorithms are then compared using various parameters like scalability, security, block size and key length . We then consider modern security schemes and cryptosystems towards effective encryption .This facilitated the study and understanding of the evolution of security algorithms for cloud security from its roots via traditional schemes to its modern day interpretations .

ACKNOWLEDGEMENT

We convey our sincere thanks to our project guide Ms. Shanthi D L who provided us with the opportunity and without whose encouragement this work would not have been possible .We would like to thank our department and college who have been very supportive .We would also like to thank our parents whose constant support and encouragement is invaluable and indispensible .

REFERENCES

[1] Md Asif Mushtaque, H, Dhiman, S. Hussain and S.Maheshwari, "Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[3] 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 .

[4] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213-229, 2001.

[5] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494, pp. 457-473, 2005.

[6] S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, "Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions," Proc. ACM Conf. Computer and Comm. Security,pp. 152-161, 2010.

[7] Cheng-Kang Chu ,Sherman S.M. Chow ,Wen-Guey Tzeng , Jianying Zhou, and Robert H. Deng "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage " , IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014 .

IJSER

[8] F. Guo, Y. Mu, and Z. Chen, ―Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key,‖ in Proceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575. Springer, 2007, pp. 392–406.

[9] Xing Zhou, Xiaofei Tang , " Research and Implementation of RSA Algorithm for Encryption and Decryption", Department of Computer Science and Technology Harbin, China , 2013..

[10] Sameer Raja, " Cloud Computing: The Fifth Generation of Computing " , International Conference on Communication Systems and Networking , 2011 .

[11] Charanjeet Kaur , Er. Gurjit Singh Bhathal ," Data Security Algorithms In Cloud Computing : A Review" , International Journal For Technological Research In Engineering Volume 2, Issue 5, January-2015 .

[12] Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

IJSER