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. 3, Issue 10, October 2015

Various Approaches on security Issues in Cloud- A Review

D.Nivetha[1], B.Muthusenthil[2]

II Year M.E Student, Dept.of CSE, Valliammai Engineering College, Chennai, India[1]

Assistant Professor, Dept.of CSE, Valliammai Engineering College, Chennai, India [2]

ABSTRACT: Cloud computing is a service oriented concept and offers a service to end users. The two benefits of cloud are low cost and ease of use and the top concerns of cloud computing are trust and security, privacy issues. The security issues in cloud computing are addressed by various standards and techniques which lacks in providing a complete solution. In cloud the privacy issues are handled and assessed by using privacy protocols and assessment techniques which are also addressed. Achieving secure data sharing is a challenge in cloud that we have to encrypt the data and should be available to those authorized clients. This is made probable through re-encryption. In re-encryption process, the cipher text encrypted under the public key is converted to a different cipher text encrypted under the receiver's public key.The secret key should not be given to the re-encrypting authority or the plain text during the process. This paper discuss about various encryption and re-encryption technique for secure data sharing.

KEYWORDS: Cloud, Security issues, Re-encryption

I. INTRODUCTION

Cloud Computing is a model which has evolved from distributed computing, virtualization technology, utility computing and other computer technologies. cloud computing provide services on virtual machines allocated over large physical pool of resources. For large enterprise level applications, scalability and availability are characterized to address. Cloud Providers maintains computing resources and data automatically via software. For the organization, the cloud offers data centers to move their data globally. Maintaining the data and also cloud supports customizable resources on the web. The data are uploaded in the cloud as encrypted form. While, sharing the data cloud should ensure that the authorized parties will get the appropriate data without any hold-up which may be incurred due to the Re-encryption process. The service models in the cloud are,

Infrastructure as a Service:IaaS offers virtualized IT resources for computing, storage and networking on demand. The user can run the application in chosen OS environment. The user has control over the OS, storage, deployed applications, but cloud infrastructure is not managed by user. In Cloud stack, its bottom layer is made of Virtualized resources. E.g. of Iaas includes Amazon EC2, Flexiscale, Joyent, GoGrid, Rackspace cloud servers [20].

Platform as a Service: To make a Cloud easily programmable, PaaS offers a higher level of abstraction. To create and deploy applications, Cloud platform offers an environment in which no. of processors or amount of memory used for those applications are not necessary .such a platform includes operating system and runtime library support. E.g. of PaaS includes Aneka, Google App Engine and Microsoft Azure.[20]

Software as a Service: software as a service refers to browser initiated applications software over thousands of cloud consumer. The SaaS model provides software applications as a service. On cloud stack, the applications are resided on the top layer and through web portals provided by SaaS, end users are allowed to access the services [20].

Depending upon the customer requirements, cloud services can be deployed in four ways in the service models as shown in Figure.1. They are,

Public Cloud: A cloud infrastructure is managed by a third party and provided to many customers[18].At the same time multiple enterprises work on the infrastructure Through Internet users can gather information about their required resources from an offsite service providers. Users are asked to pay for whatever they use and the wastage of resources is checked to avoid it in future.

Private Cloud: Only a specified customer is allowed to work on Cloud infrastructure which is managed by a third party service provider [11]. Virtualization of machines is the concept used in private cloud and it is a proprietary network.

Community Cloud: Many organization shares cloud infrastructure and supports a specific community. The organization in community cloud is managed and operated by sharing common goals. It may exist on or off premises.
Hybrid Cloud: For data transfer, two or more cloud deployment models are linked in. While data transferring, cloud deployment models are not affected by each other [24].

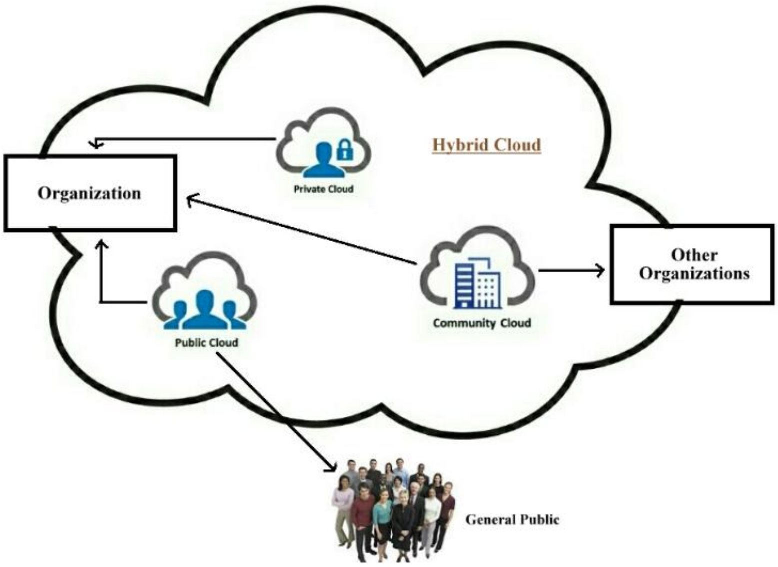

Figure.1.Cloud Deployment Models

The security requirements in service-oriented cloud computing model are as follows:
Data Security: Security measures should be taken by the service provider to protect client's data and applications and it is ensured by the customers that their information are protected.
Privacy: Only authorised users are allowed to access the system. The digital identities and credentials produced by the customers are collected by the provider and they should ensure that the infrastructure is secure. The provider collects or produces about customer activity in the cloud.
Data Confidentiality: The cloud provider should protect the data given by the customers and they should make ensure that their information is confidential from the potential competitors[18].
Fine grained access control: A set of users are allowed to facilitate granting differential access rights which provides flexibility in specifying the access rights of individual users. Encrypting data by using certain encryption techniques is the effective implementation for fine grained access control in a feasible way.

II. VARIOUS ISSUES IN CLOUD

A. *Security Issues:*

The techniques which are used to eliminate security issues are 1) Identity and access management[26,21] 2) Data security[14]. and 3) Trust and assurance. Federated Identity Management (FIM) is a technique followed by IAM technique. FIM technique provides identities of information that is distributed across multiple parties and security domains. In cloud services, security issues raises due to its sharing nature. It leads the individual user to lack the control of different technology stacks because of data centric property.

B. *Risk Management Issues:*

In order to identify, monitor, assess and manage the systems uses a typical risk management system in a proactive way. Based on the risk assessment it categorises the business risk model. An authenticated user can access the customer's private data to prevent from unwanted access. The cloud services should be available all time as 24/7 without any unavailability issues. According to customer's demand the resources are increased and decreased in cloud services. Amazon EC2 data centres became static nearly up to 4 hours due to lightning strike in June 2009. Design of an underlying cloud infrastructure is made in a flexible and scalable manner. According to customer's demand they can choose bandwidth, speed and response time [27].

C. Access Level Issues:

The people use variety of devices which is used to access cloud because they are in unsecure remote location. Since the people are from same organisation so they obey the corporate guidelines and standards. Thus data security and usage issues exist. The employees use their own devices to share their data with their friends and colleagues. Thus data from other organisation is shared it affects great security breach and it may leads to loss of corporate standards[22].

D. Trust Model Issues:

PKI based trust model: The process is based on community principles and verification authentication authority. Normal authorities are suitable only for community whereas PKI is suitable for more number of authorities. The participants who have the high security level is allowed to have an authority key will be handled by trust mechanisms namely out-of-band mechanisms, trust lists certificate, request messages certificate and cross-certification [5].

Feedback creditability based global trust model: It is an adaptive topology for an unstructured P2P networks. It is used to find out relationship between the trusted peers and keep away the untrusted peers[16].

Behavioural based trust model: Behaviour is a factor used by security model, which uses various domains with different context. Direct trust and Indirect trust are the two trust types which is implemented by a modern trust model[12].

Subjective trust model: In this model the trust decisions are identified over internet environment and classified as a trust subjects by using the decision constraints. In order to reduce the hazards from malicious node, the subjective trust management model has been implemented in the MANET with various decision factor[31,13] .

Domain-based Trust Model: The large scale peer-to-peer network suffers in establishing trust relationship among the peers with frequent interactions. Each peer-to-peer network is assigned by a super node which holds all domain specific entities from other peers. There are two ways to establish the trust namely 1) between entities and domain 2) between the domains [8]. In homogeneous environment, these models are suitable to apply which will be extended to the cross-cloud environment over large scale and complex application which raises in a security risks .

III. Approaches To Security Issues In Cloud

A. Dynamic Substitution Method:

Substitution is made static and each time a value occurs, the same output value is generated by the encryption algorithm. In the processed data the probabilistic distribution of the information source is maintained and it provides valuable clues to attackers. During the substitution stage , some uncertainty must be introduced. The uncertainty is made by using a pseudorandom sequence and it is controlled by a component of the encryption key. To the input data the noise is added by using the addition rule of the algebraic finite field and defined as:

$$s = a + n$$

s isthe output sequence; a the input data sequence and n a pseudo-random sequence. The correlation between the input data symbols and the output sequence are to be minimized[29].

B. Public Key Cryptosystems:

Messages are encrypted and decrypted with two different keys in such a way that it is difficult to decrypt without the decryption key. Without compromising security the encryption key can be broadcasted and called as public key ,the decryption key is called the private key. In a public-key cryptosystem the encryption and decryption key differ, such systems are often called asymmetric. Confidentiality and key management are provided by public key cryptosystems. Public key cryptosystems are more secure than secret-key cryptosystems, but they are generally slower. Their main advantage is secret key is not agreed to the parties. Although there is no standard public-key cryptosystem, many consider a cryptosystem invented by Rivest, Shamir, and Adleman (RSA) [25] in 1977 a de facto standard. Public-key cryptosystems, like secret-key cryptosystems, are rarely standardized.

Digital Signature:

Messages are signed and verified by the resulting signature with twodifferent keys in such a way without the signing key it is difficult to sign. Like, public-key cryptosystems, the verification key can be broadcasted, and is called the public key; the signing key is called the closely related. In reversible cryptography, signing in a digital signature scheme is the similar to decryption in a public- key cryptosystem, while verification is the same as encryption. In irreversible cryptography, the public/private-key pair may work in both a digital signature scheme and a public-key cryptosystem. There is no standard digital signature scheme, but two main efforts are in progress. One involves RSA, which is reversible, and the other is an irreversible algorithm proposed by the US National Institute of Standards and Technology (NIST). The standard for RSA, is created by ISO/IEC 9796 [15] but not quite.

Elliptic Curve Cryptography:

Current public key cryptosystems are mainly public key cryptosystem based on error correction code, Goldwasser-Micali probability public key cryptosystem, Merkle-Hellman knapsack public key cryptosystem, ElGamal public key cryptosystem, Rabin public key cryptosystem, elliptic curve cryptosystem, and finite automaton public key cryptosystem, et.al. The fundamental idea of elliptic curve cryptography is to transfer the discrete logarithm problem that existed several hundred years ago to elliptic curve for its implementation. Two difficult mathematical problems involved by public key cryptography when put forward initially are: 1) factors decomposition problems; 2) discrete logarithm problem. In the situation that the computing ability is improving continuously currently, the solution to discrete logarithm in common mathematical sense becomes a relatively easy job. Therefore, consider transferring the solution of discrete logarithm problem to a more difficult field to implement and then it is transferred to elliptic curve. Elliptic Curve Cryptography (ECC) is to transplant original encryption algorithm to elliptic curve. It not only realizes key exchange protocol and public key encryption and decryption, but also realizes digital signature. The essence of ECC is to transplant classical encryption algorithm to secure elliptic curve for its implementation. For example, in RSA, they are common modular addition, modularmultiplication previously; now after it is transplanted to elliptic curve, they become point addition and point multiplication, which are also called elliptic addition, ellipticmultiplication. Additionally, modular reduction is to limit it in the range between 0 and n-1 [28].

RSA Encryption:

The most successful, asymmetric system in the present criteria is RSA Encryption system. Its Cryptologists Rivest, Shamir and Adleman make an attempt to break another cryptographic problem. RSA works with two different keys: Public key and a Private Key. Both the keys work complementary to each other. If a message is created by a public key, it can be decrypted by a private one. From public key, private key cannot be calculated. Thus latter is made available to public key. By these properties, it is allowed to use asymmetric cryptosystems in a wide array of functions, known as digital signatures. Instead of signing the document, RSA provides a Fingerprint encrypted and enables to verify both the sender and integrity of the document by the receiver. RSA security is based mainly on mathematical problem of integer factorization. At current, it cannot able to calculate numbers greater than 768 bits. 3072 bits is a minimum key length used in modern cryptosystems.

C. Secret Key Cryptosystems:

Messages are encrypted and a decrypted with a key in such a way that it is difficult to decrypt without the key. In a secret-key cryptosystem encryption and decryption keys are same are, such systems are often called symmetric in the literature. Most secret-key cryptosystems operate on messages one block at a time; a block may be 64 bits long, and the keys are usually short, say, 56 bits long. Secret-key algorithms are generally quite fast. Secret-key cryptosystems, the secret keys are agreed to the parties and provide confidentiality, key management to those parties. The primary standard is the Data Encryption Standard (DES) which is published in 1977 and recently affirmed for a fourth five-year period, DES defines the Data Encryption Algorithm (DEA). DEA is specified by ANSI standard X3.92[1] and Australian Standard AS2805.5.The Data Encryption Algorithm seems to be quite secure, as far as 56-bit algorithms go. It resists powerful attacks that have broken other systems[3,6]. Along with DES the standard modes of operations are electronic codebook, cipher block chaining, cipher feedback, and output feedback. These modes are applied to any block cipher. ANSI X9.17[2] introduces the encrypt- decrypt-encrypt (EDE) mode of encryption involving two DEA keys.

AES Encryption:

Block cipher is the data blocks of 16 byte in which the algorithm is executed. It is based on several substitutions, permutations and linear transformations. It is repeated several times and it is called by a term “Rounds”. A Unique round key is calculated during each round. . Based on the AES block structure, the change of a single bit either in the key, or in the plaintext block results in a different cipher text block – a clear advantage over traditional stream ciphers.AES-128, AES-192 and AES-256 has difference in length of the key. Because of its highly secured model, AES is the standard encryption for governments, banks and highly security systems all around the world.The AES cipher has,

1.Substitute bytes transformation.
2.Shift rows transformation.
3.Mix columns transformation.
4. Addround key transformation.
5.AES key expansion.

DES Encryption:

In DES, message is encrypted and decrypted by using the same key a message, so both the sender and the receiver must know and use the same private key. The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm is applied to a data block simultaneously rather than one bit at a time. DES groups it into 64-bit blocks to encrypt a plaintext message. By using the secret key each block is enciphered into a 64-bit cipher text by means of substitution and permutation. The process involves 16 rounds and can run in four different modes, blocks individually encrypted or making each cipher block dependent on all the previous blocks. The inverse of encryption is decryption, but reversing the order in which the keys are applied.

Blowfish Algorithm:

Blowfish has a 64 bit block size. The variable key length is from 1 bit to 448 bits. It uses large key – dependent S boxes and it is a 16 round feistel cipher. CAST-128 uses fixed S- boxes and the structure of blowfish algorithm resembles it. 18-entry P-array and four 256-entry S-boxes are the two sub key arrays used by the algorithm.

The literature survey of various encryption techniques is described in Table.1 as follows,

Table.1 Various Approaches On Cloud Security Issues

PUBLIC KEY CRYPTOSYSTEM			
Method	**Author**	**Year**	**Remarks**
New directions in cryptography	Rivest,Shamir,Adelman	1978	It provides confidentiality and key management. More secure than secret key cryptosystem. Public cryptosystem is invented by RSA[7].
Quantum cryptography	C.H.Bennett	1984	Quantum cryptography not based on mathematical one way function[4].
Survey on public key cryptosystem	Neal Koblitz	2004	Diffie and Hellman invented a new cryptography called public key using a one way function for encryption.
ELLIPTIC CURVE CRYPTOGRAPHY			
Methods for index computation	J.M.pollard	1978	Endomorphism not only speed up scalar multiplication they also speed up pollarids rho algorithm[23]
Selecting smaller key sizes	A.k.Lenstra	2001	Elliptic curve cryptography offer small key size[17]

Copyright to IJIRCCE
DOI: 10.15680/IJIRCCE.2015. 0310021

Elliptic curve algorithm integration in the secure shell transport layer.	D.stebila	2009	RFC 5656 specifies the elliptic curve diffie hellman key exchange method[30].
Identity based elliptic curve signature in tripartite key exchange protocol	Jia Zfao	2012	In this paper proposed an Id based elliptic curve signature algorithm.
DIGITAL SIGNATURE			
Digital signature standard	Federal Information Processing Standards	2000	Digital signature is computed using factorization problem[9]
Digital signature	Chang	2004	Digital signature scheme based on public key cryptosystems are vulnerable to existential forgery attack.
Fast ECC Digital signature based on Dsp	Yin Qin	2012	In this paper proposed an variable window mechanisms
RSA			
Twenty years of attacks on the RSA cryptosystem	Dan Boneh	2000	RSA is classified into traditional mathematics attacks and implementation attacks[10].
RSA speedup with Chinese Remainder Theorem immune against hardware fault attack	s.yen	2003	Chinese R3minder theorem based on RSA used to speed up the decryption and signing process in multi prime RSA.
File Encryption and Decryption Using Secure RSA	Rajan.S. Jamgekarr	2013	RSA is used in encrypted connection, digital certificate algorithm
ELGAMAL CRYPTOSYSTEM			
A public key cryptosystem and a signature scheme based on discrete logarithms	TaherElGamal	1998	Elgamal algorithm is a public key cryptography based on discrete logarithms problems.
File Encryption and Decryption Using Secure RSA	Rajan.S. Jamgekarr	2013	The exchange of secret key elgamal encryption is used in GNU privacy guard software.
DATA ENCRYPTION STANDARAD			
Superior Security Data Encryption Algorithm	Yashpal	2012	TDES is a block cipher formed from DES cipher.
A Survey on Various Most Common	G.Ramesh	2012	TDES require more time than DES.

Encryption Techniques			
Survey of Various Encryption Techniques for Audio Data	Manpreet Kaur	2014	DES is block cipher based on symmetric algorithm.
ADVANCED ENCRYPTION STANDARD			
AES	Xinniao zhang	2002	Various approach for efficient hardware implementation of AES algorithm
BLOWFISH AND AES	Milind Mathur	2013	It uses variable length key of size 128,192,256 bits[19].
AES in computer and network security.	Avinash Kak	2015	AES focus particularly on byte substitution, shift rows, mix columns, add round key.

IV. Re-encryption Techniques

A. Reliable Re-encryption In Unreliable Clouds:

Due to unreliable network communication commands may not receive and executed by all cloud servers. It is because; the cloud computing environment is comprised of many cloud servers. By proposing a time based re-encryption scheme, the problem can be solved. It enables the cloud servers to automatically re-encrypt data. It is based on their internal clocks. Attribute based encryption (ABE) scheme is used as a platform and the solution is built on its top. Using an access structure comprised of different attributes, ABE allows data to be encrypted. Without receiving any command from the data owner, each cloud server will independently re-encrypt data. In this scheme data and keys are not shared. It provides,

1. Time based re-encryption,
2. Attribute Based Encryption,
3. User revocation,
4. Data confidentiality and efficiency.

B. Quorum Controlled Asymmetric Proxy Re-encryption:

If there is no dishonest quorum of proxy servers, then the re-encryption is secure for so long in this scheme [30]. In multiparty communication, it is an efficient method. Because it transforms encrypted message to recipients with different public keys. Gradual and simultaneous process is carried out by the mentioned re-encryption scheme. A unit of operation which is the combination of one partial encryption by private key and one partial encryption by a public key is performed by each proxy server. Gradually this process is carried out all the proxy servers. If plain text is not obtained in the operation, then the system is secured. Anyone can verify the accuracy of the method without knowledge of private key of recipient using translation certificate. This scheme provides,

1. Asymmetric re-encryption,
2. Private Key is shared as quorum,
3. Verifiable translation certificate.

C. Improved Proxy Re-encryption Scheme:

Bilinear maps are considered while enhancing this scheme. Customized encryption process is carried out. The sender is given a choice to set the recipient using the same public key. Using receiver's public key re-encryption are generated by the sender. It is a collusion resistant algorithm. This scheme provides,

1. Asymmetric re-encryption.
2. Non interactive.
3. Unidirectional.
4. No secret key pre-sharing needed.

V. CONCLUSION

The cloud service models are used to provide various services which are suitable for the cloud customer. These services are deployed in the model which depends on the factors such as boundary, location, security, privacy, storage, identity etc. The community cloud, public cloud and hybrid cloud are facing a problem in handling the above factors. The cloud issues like security issues, risk management issues, access level issues are also identified. This paper contains several encryption and re-encryption algorithm for secure data sharing in cloud server. From the survey we understand that some amount of work has been done in the field of cloud computing for several security issues.

REFERENCES

[1] Accredited Standards CommitteeX3,ANSlX3.92: Data Encryption Algorithm (DEA), ANSI, New York, 1981.

[2] Accredited Standards CommitteeX9, American National Standard X9.17: financial Institution Key Management (Wholesale), ANSI,1985.

[3] E. Bihamand A. Shamir, "Differential Cryptanalysis of theFulll6- Round DES," *Proc.* Crypto 92, Advancesin Cryptology, Springer- Verlag, New York, 1993.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing",IEEE International Conferenceon Computer Systems and Signal Processing, Bangalore India, pp. 175-179, 1984.

[5] Changping Liu,Chengdu, Yong Feng, Mingyu Fan, Guangwei Wang, "PKI Mesh Trust Model Based on Trusted Computing",IEEE 9th International Conference for Young Computer Scientists,PP.1401 -1405 ,2008

[6] D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength Against Attacks",IBM J. RES, DEVELOP, VOL. 38 NO. 3,PP.243-250,1994

[7] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, pp. 644-654,1976.

[8] Fen Xu,Yajun Guo,"A Domain-Based Trust Model in Peer-to-Peer Environment", International Journal of Distributed Sensor Networks,Volume 5, Issue1,PP.1-15 ,2009

[9] "DIGITAL SIGNATURE STANDARD (DSS)", Federal Information Processing Standards Publication 186-2, 2000.

[10] Dan Boneh, "Twenty years of attacks on the RSA cryptosystem," 2000.

[11] R. L Grossman, "The Case for Cloud Computing", IT Professional, vol. 11(2), pp. 23-27, 2009.

[12] Gui Xiaolin,Xie Bing, Li Yinan, Qian Depei," Study on the behaviour based trust model in grid security system", IEEE International Conference on service computing,PP. 506 -509 ,2004.

[13] Hui Xia1,Zhiping Jia1,Lei Ju1,Xin Li,Youqin Zhu, "A Subjective Trust Management Model with Multiple Decision Factors for MANET basedon AHP and Fuzzy Logic Rules", IEEE/ACM International Conferenceon Green Computing and Communications,pp.124-130,2011.

[14] Information Supplement: PCI DSS Cloud Computing Guidelines,*Information Supplement, PCI DSS Cloud Computing Guidelines* , PP 1-50 ,2013

[15] International Standard 9796: Information Technology, Security Techniques: Digital Signature Scheme Giving Message Recovery, ISO/IEC, 1991.

[16] Jianli Hu, Quanyuan Wu, Bin Zhou, TTEM:" An Effective Trust-Based Topology Evolution Mechanism for P2P Networks",JOURNAL OF COMMUNICATIONS, VOL. 3, NO.7, PP.3-10 ,2008.

[17] A. K. Lenstra and E. R. Verheul." Selecting cryptographic key sizes", Journal of Cryptology, PP.255-293,2001.

[18] Michael Armbrust, Armando Fox, Rean Griffith,Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee,David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia."A view of cloud computing",Communications of the ACM,Volume 53, Issue. 4, PP.50-58,2010.

[19] Milind Mathur, Ayush Kesarwani "Comparison between DES, 3DES, RC2, RC6, BLOWFISH AND AES",Proceedings of National Conference on New Horizons in IT - NCNHIT ,PP.143-148,2013

[20] "National Institute of Standards and Technology", NIST Definition of Cloud Computing, 2011.

[21] "Novell, Identity and Access Management in the Cloud", Cloud Security Alliance Research Paper, PP.1-41,2010.

[22] Piers Wilson," Positive perspectives on cloud security", Information security, PP.1-5,2011

[23] J. M. Pollard,"Monte Carlo methods for index computation (mod p", Mathematics of Computation, PP.918-924, 1978.

[24] Rohit Bhadauria et. al. paper on "A Survey on Security Issues in Cloud Computing".

[25] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems",*Comm.* ACM, Vol. 21, No. 2, pp. 120-126,1978.

[26] Sally Hudson," Better Identity and Access Management in the Age of Cloud Computing", IDC ANALYST CONNECTION, PP.1-4 ,2012

[27] Scott Paquette, Paul T. Jaeger, Susan C. Wilson, "Identifying the security risks associated with governmental use of cloud computing", GovernmentInformation Quarterly ,PP.245-253 ,2010

[28] SU He-peng,ZHANG Sheng-bing. "Design and Implementation of an Architecture of Multi-Scalar Multiplication for ECC Based on Binary Edwards Curves",Microelectronics & Computer,PP.98-102,2011.

[29] L. Scripcariu, A. Alistar, M.D. Frunza, "JAVA Implemented Encryption Algorithm", Proc. of the 8th Int. Conference Development andApplication Systems, Suceava, pp. 424-429, 2006.

[30] D. Stebila and J. Green. "Elliptic curve algorithm integration in the secure shell transport layer". RFC 5656,PP.1-20 2009.

[31] Shouxin Wang,Li Zhang,Na Ma,Shuai Wang, "An Evaluation Approachof Subjective Trust Based on Cloud Model" ,Journal of SoftwareEngineering and Applications, PP.44-52 ,2008.