ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 12, December 2016

Secure Data Sharing Through an Integrated Encryption System in Cloud Computing

Sudheer Kumar Arya*[1] Palak Shrivastava2 Priyanka Tripathi[3]
National Institute of Technical Teacher's Training & Research
Bhopal

Abstract
Latest technological trend of computing over internet is, the Cloud Computing. Cloud consist thousands of network that require enhanced security and authorized access in it while Data Sharing. The authors in this paper have analyzed various issues, models, and techniques on secure data sharing in their survey. Further based on the critical observations authors have suggested a novel methodology for more secure Data Sharing in Cloud Computing. This proposed methodology is also analyzed under certain factors by the authors for proving its efficiency.

Keywords

Elliptic Curve Encryption, Cloud Computing, Cryptography, Data Sharing, Integrated Elliptic Curve Encryption System

I. INTRODUCTION

Cloud Computing is the term which is very famous these days in field of technology where all technical devices are linked and synchronized according to it. Cloud Computing is used for online storage which is based on single click operation by a user sitting anywhere around the globe. The qualitative services from configurable computing resources, without the overwhelming efforts of local data storage and maintenance are in the main demand of the market. Over internet thousands of networks are interconnected that require enhanced security and authorized access in it. While sharing of the data the authorization and confidentiality parameters require major concern. So this paper focuses on enabling secure and confidential sharing of data using cloud computing technology. For single click easy and secure transfer of information in cloud computing the concept of encoding the data in a particular format on the sender side and then decoding it in a readable format on receiver side is taken into consideration which in general called as Cryptography. By deploying this concept the highly secure and well authenticated sharing of data is achieved when it is mixed with the proposed approach of obtaining attributes from an elliptic curve integrated system.

This paper thus presents Integrated Elliptic Curve Encryption scheme to enable highly secure and confidential sharing of data using Cloud computing technology. It also highlights the contrast between the existing Revocation Scheme based on

Proxy Re-Signature approach and the proposed Attribute based Elliptic Curve integrated system approach and thereby prove the efficiency of this work. The examples of cloud computing can be seen from daily life like the Google drive that is being used for storing personal data or information. Yahoo email, Gmail, Hotmail, Adobe are some other examples of cloud computing. Websites uses API links stored in cloud for viewing their holding content to user with special function. Cloud service provider like Amazon, Google, and Yahoo handle and manage information software and the server. Amazon was the first to provide cloud services to users, with Amazon Simple Storage Service (Amazon S3). The other providers include Apple, Cisco, Citrix, IBM, Joyent, Google, Microsoft, Rackspace, Salesforce.com and Verizon/Terre mark. The following figure displays about the a scenario in cloud computing where applications, platforms of different types works in coordination with each other to provide services to remote as well as local places. Below is the figure that displays the view of a typical cloud computing environment where sharing of information takes place everywhere:

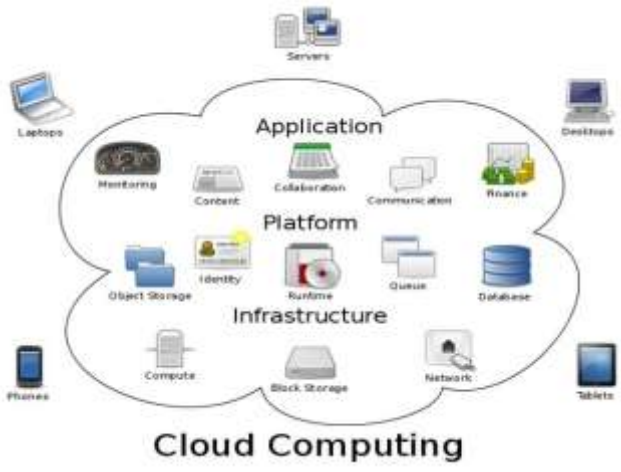

Fig 1.1: A Typical Cloud Computing Environment

Data Sharing using Cloud computing in today's life has a vital role ranging from a kid playing online games to an old retired person interacting to world via social networking sites. The extent of cloud is also to the students gaining knowledge from it to an adult utilizing cloud and sharing big data of its business. Various data storage and sharing services available today make people to easily work as a group by sharing data with each another. Once a user shares data in the cloud, the other member users in the group can not only access and modify shared data, but could also share the versions of the shared data with the group [1, 2, 3, 4]. Cloud computing being latest and unparalleled technology stores information and direct it between numerous strategies via a network by using the concepts of processing power [5, 6, 7]. Thus this paper focuses on secure data sharing using cloud computing technology.

II. LITERATURE SURVEY

To enable data sharing in the Cloud, it is imperative that only authorized users are able to get access to data stored in the Cloud. The ideal requirements of data sharing in the Cloud includes that the data owner should be able to specify a group of users that are allowed to view shared data. Any member of the group should gain access to the data anytime without the data owner's intervention. No other user, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The secure data sharing is obtained by the concepts of cryptography that basically the two processes of encryption and decryption. After implementation of public key cryptography by Diffie and Martin in 1976 [8, 9, 10], several cryptosystems have been proposed. So in place of DES (SKC) the algorithms like ECC, RSA (PKC) is used for secure communication. In 1985, Victor and Miller independently proposed a cryptosystem based on elliptic curves defined over finite fields, based on DH key exchange protocol whose security relies on the elliptic curve discrete logarithmic problem (ECDLP). ECDH key exchange scheme analog of DH key is for communicated securely over insecure channel means no prior contacts between parties. Parties generates a public and private key respectively and exchange public keys, then combines its private key with the other party's remote key to form the secret shared key. By exchanging of secret key primarily in communication, and provide data confidentiality and integrity. In comparison with other cryptosystems like RSA, Elliptic Curve Cryptography uses significantly shorter keys which help to provide easier data management, lower requirement of data space, less bandwidth over network and longer battery life for devices like smart phones.

A. Elliptic Curve Encryption Scheme in Data Sharing Environment

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations [11]. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography. The mathematical operations of ECC is defined over the elliptic curve [12, 13, 14],

$$\mathbf{y^2 = x^3 + ax + b}$$

where, $4a^3 + 27b^2 \neq 0$.

Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its small key size. A 160-bit key in ECC is considered to be as secured as 1024bit key in RSA. Elliptic Curve Cryptography (ECC) is emerging as an attractive public key cryptosystem, in particular for mobile (i.e., wireless) environments. Elliptic Curve Cryptography (ECC) offers smaller key sizes, faster computation as well as memory, energy and bandwidth savings and is thus better suited for small devices Koblitz and Miller independently published work on ECC in 1985 for the first time [15, 16, 17, 18].

ECC operates on groups of points over elliptic curves and derives its security from the hardness of the elliptic curve discrete logarithm problem (ECDLP) [19, 20, 21, 22]. This dissertation relies on Integrated Encryption Scheme (IES) is a type of elliptic curve encryption scheme based on attributes obtained from an ellipse which is an integrated system that provides secure data sharing while maintaining data confidentiality, integrity, authorization as well as security.

The main objective of this literature review is to find the gaps in research work and formulation of problem on which this work is based. Some of the referenced papers have been reviewed below.

Boyang Wang et al. [23] research that proposed the system model which comprises three objects: the mist, the third party auditor (TPA), and users who share data as a group. The cloud offers data storage and sharing services to users. The TPA is able to publicly audit the honesty of communal information in

the cloud for users. In a group, there is one original user and a number of group users. The original user is the original owner of data. This original user creates and shares data with other users in the group through the cloud. Both the unique worker and collection users are able to admission, transfer and adjust common information. Communal information is additional alienated into a quantity of chunks. To protect the truthfulness of communal data, each chunk in common data is attached with a signature. Such a representation is showed in the following figure 1.2

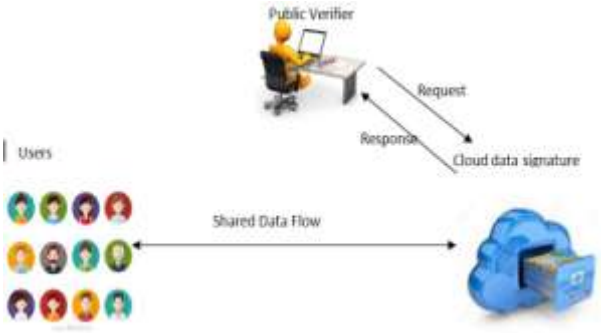

Figure 1.2 System Model

Similarly Zhao et.al [24] proposed a progressive elliptic curve encryption scheme (PECE) whereby a portion of data is encrypted a number of times using multiple keys and later decrypted using one key. Data sharing involves one user encrypting its data using private key and storing the encrypted data to the Cloud. Another user sends request for data access permission by sending his public key to first user which sends a credential to the storage provider for re-encryption of data. This is an effective technique as it keeps data confidential as data is encrypted throughout the entire stages thus never allowing a malicious user to view the plaintext data.

Goyal et al. [25] proposed Attribute-Based Encryption (ABE) technique that is used to provide fine-grained access control to the data in the Cloud. Initially, access to the data in the Cloud was provided through attribute. An access control policy is defined and if the attributes satisfy the access control policy the user should be able to get access to the piece of data.

Wang X et.al [26] proposed Proxy Re-encryption is another technique that is for enabling secure and confidential data sharing in the Cloud. Proxy Re-encryption allows a semi-trusted proxy with a re-encryption key to translate a cipher text under the data owner's public key into another cipher text that can be decrypted by another user's secret key. At no stage will the proxy be able to access the plaintext.

Yu et al. [27] proposed Attribute-Based Encryption and Proxy Re-encryption used as a hybrid of each other to provide extra security and privacy for data sharing in the Cloud. The scheme works by data owner encrypting its data using a symmetric key and then encrypting the symmetric key using a set of attributes according to KP-ABE scheme.

Shucheng Yu et al. [28] proposed the scheme which enables the authority to revoke any attribute of users at any time while placing a minimal load. It provides the definition for attribute revocation with severs.

Alexandra Boldyreva et.al [29] proposed Identity-based Encryption with Efficient Revocation. It is an exciting alternative to public-key encryption, as IBE refrain from the need for a Public Key Infrastructure (PKI). Any setting, PKI or identity-based, must provide a means to revoke users from the system.

Autade Dhanshri et.al [30] proposed group user revocation for securely sharing the data file among the dynamic groups without revealing their identity members. The revocation will be forwarded to the auditor where auditor will check to it. A system model for the cloud storage architecture, which includes three main network entities: users, a cloud server, and a trusted third party as shown in figure 1.3:

Figure 1.3 Group User Revocations for Shared Dynamic Cloud Data

Michael Cobb [31] this is the article which shows the comparison of the nature of the Diffie-Hellman key exchange that tells about weakness in susceptible to man-in-the-middle attacks since it doesn't authenticate either party involved in the exchange. So the reason of, Diffie-Hellman to be used with a combination of an additional authentication method is with the gital signatures. When using RSA, a 1,024-bit key is considered suitable both for generating digital signatures and for key exchange when used with bulk encryption, while a 2048-bit key is recommended when a digital signature must be kept secure for an extended period of time, such as a certificate authority's key.

Jueles, Kaliski et.al [32] proposed the scheme for store the data files in unstructured storage for sampling block of files randomly based on homomorphism linear authenticator works on RSA. But there is lack of data security to eavesdropper.

Mohta, Awasti et.al [33] proposed scheme that provide security that works on short signature techniques based on Diffie Hellman algorithm elliptic curve and hyper elliptic

algorithm. With half length of signature provide secure level of sharing. The fault of Diffie Hellmann and DSA algorithm provides key management and authenticity respectively.

Menezes Qu Vanstone et.al [34] proposed the schemes of elliptic curves which is started from variant of ElGamal, the improved security in data sharing is achieved by masking the message in plain text and each message is match with the point in curve. Using this cryptosystem, it is possible to divide any plaintext in blocks, and each block is encoded as ordered pair. These elements consist of elements in finite field. Since the encryption of the information generates cryptograms that are much larger than other algorithm, Kiefer shows in this cryptosystem in insecure.

R. Cramer et.al[35] proposed a scheme in which the four public key is used that consists of points on elliptic curve, it uses key derivation function first coordinate of a point of curve made by calculation for encryption process. In key generation process, uses two additional elliptic curve points to secure data sharing.

V. Martinez et.al [36] proposed new elliptic curve scheme integrated encryption scheme, the scheme is based on the elliptic curve finite field in which the recipient choose randomly one public key and the private key is chosen individually, the complete process of data sharing is derived by using hash function, key derivation function, key agreement between recipient and message authentication code for user. Then, use of this scheme in java card is implemented and the limitation of functions availability is verified. The various version of this scheme is also included.

III. PROPOSED METHODOLOGY

The detailed literature survey has yielded identification of certain gaps in the research domain. Those gaps have been formulated into specific problems in accordance with the existing methodology implemented for the data sharing over clouds. The scenario contains following issues that need to work upon:

- The feature of data sharing over cloud should be more secure and efficient where computational overhead of the algorithms must be as low as possible. This in turn also means that integrity of data is not ruined while delivering and it is being delivered only to the authenticated user.
- The large sized keys for encryption and decryption creates the issues of cost and effective management. Therefore the problem of complex system deployment must be avoided.
- The inefficient revocation and more revoked user for per auditing tasks is the another major issue that needs to be concentrated upon.
- The issue of computational time where revocation, auditing time, revocation with verification time is still untouched factor that needs to be worked on.
- Deploying all these features in a cloud computing where thousands of networks are interconnected is also among the gaps which have been identified.

The proposed approach can be considered as a framework model for creating simulation environment and then to effectively share the data over clouds following steps are followed:

A. Creation of Integrated Elliptic Curve Encryption System

This dissertation thus with the aim of efficient revocation of users and enhancement in factors like auditing time, revocation time etc with respect to increased number of users, while handling various security issues presents the scheme of Attribute based elliptic curve encryption which works in following manner. The proposed methodology works under the following phases in which following phases happens in one single system as shown in figure 1.4:

i. Creation of a cloud simulation environment.

ii. Registration of users on the simulated clouds for effective data sharing.

iii. Generation of group signatures by public verifier for maintaining authenticity.

iv. Encryption of data for secure data sharing to the members of the group using the IECES.

v. Decryption of data to obtain the validated data among the authenticated member of the group.

As shown in the figure 1.4 the proposed methodology describes the total sequence whereby a central authority is in direct contact with the storage site that defines attributes that are actually the base points selected from a elliptic curve and are uniquely defined. The encrypt section defines the combinations that are being defined by the attributes and a set of steps being described in the proposed methodology. The cloudlets contain thousands of receivers that are being registered in the group by a membership registration process and are provided with the set of base point for the generation of their public keys. On the other side while decrypting combination of common base point with the public key and private key authenticated user decrypts the data. The following algorithm is followed for the efficient and secure data sharing that maintains its integrity and confidentiality.

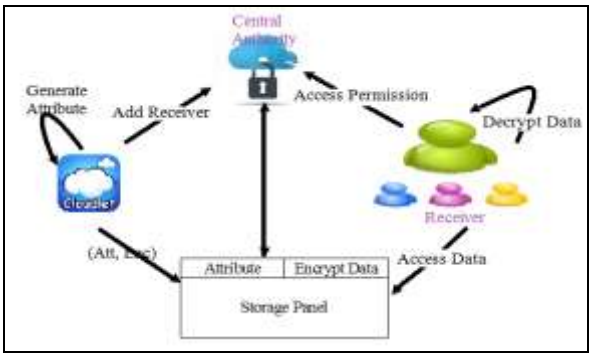

Figure 1.4 Proposed Methodology

The algorithmic steps for encryption scheme are:

Algorithm for Encryption

For sharing securely any message M with the public key Y follow the steps (i) to (vi) for encryption
(i) Register in the group through the button click operations and enter in a specific group to obtain a group signature.
(ii) Check if
Login= =Successful && Signatures= =.Verified
Else
End
(iii) Store the common base point obtained from the elliptic curve and compute the public key U and private key U' for both sharing and retrieval,
U = X.G && U'=X'.G, where X= private random number and G = common base point
(iv) Calculate key derivation function (KDF) for both sharing and retrieval denoted as
k1‖k2 = KDF(U ,l) where l = Length of the message
(v) Encrypt the message through the XOR based encryption operation
C = E[k1(M)], where C= Cipher Text, k1= key derivation function
(vi) Compute the message authentication code r through hash function MAC
r =MAC k2 (C), where C= Cipher Text, k2= key derivation function
(vii) Store the values in the storage site.
(viii) Share the message with (U, C, r).
End If
End

Similarly the steps for retrieving the message securely the algorithmic steps for decryption are as follows:

Algorithm for Decryption
For securely retrieving the message M with the public key Y follow the steps (i) to (vi) for decryption (i) Check if Login= =Successful && Signatures= =.Verified Else if End. (ii) Check (U, C ,r) and compute the key T T = X'.U, where X'= private key and U= public key (iii) Calculate key derivation function (KDF) denoted as k1‖k2 = KDF(U ,l) where l = Length of the message (iv) Decrypt the message through the XOR based decryption operation M= DK k1 (C), where M= Message, C= Cipher Text, k1= key derivation function (v) Compute the message authentication code r and r' through hash function MAC r =MAC k2 (C) && r' =MAC k1 (C), where C= Cipher Text, k1and k2 = key derivation functions (vi) Check if, r = r' Else if End Else if

(vii) Retrieve the message M.

End If.

End.

IV. Result Analysis

The above work of he methodology yielded many results when it implementeed in the software framework. The snapshots of the results are as follows. The existing technology of secure data sharing with the help of proxy re-signatures and proposed integrated system following analysis has been done which has proved the efficiency of proposed novel approach. The figure 1.5 displays such scenario:

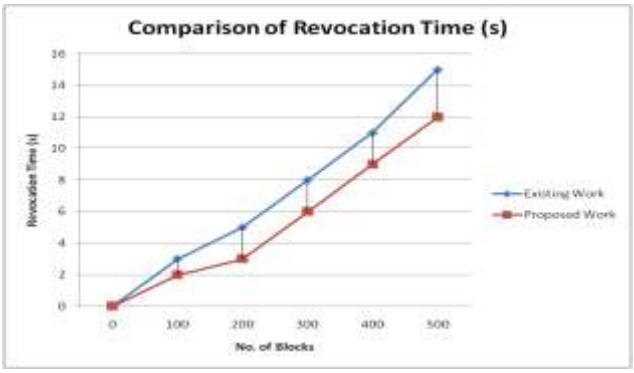

Figure 1.5: Comparison of Revocation Time

Below the figure 1.6 displays the analysis of auditing time of the proposed and existing approach:

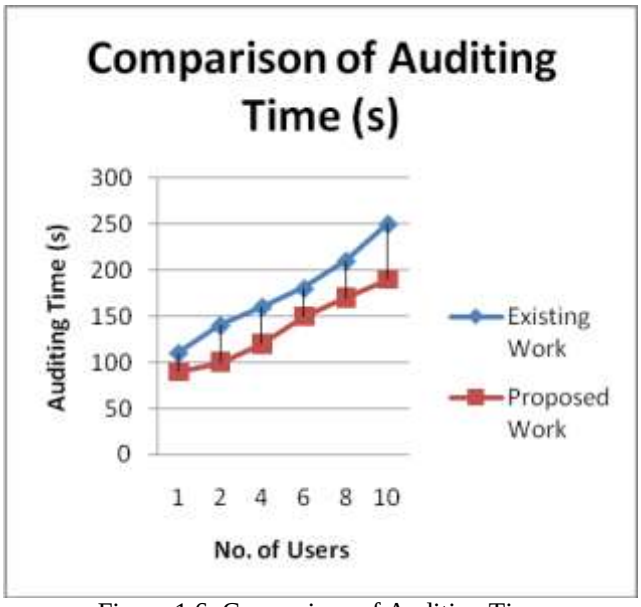

Figure 1.6: Comparison of Auditing Time

The figure 1.7 below describes the comparison of communication costs of both the approaches:

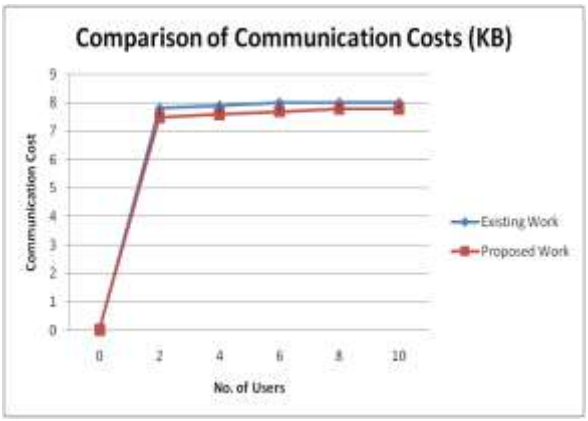

Figure 1.7 : Comparison of Communication Costs

V. Conclusion

In this paper the concept of elliptic curve encryption scheme with the attribute based scheme which work on the XOR encryption method is described. Also this paper defines the efficiency of this work by displaying the results. The authors have critically examined the issues and suggested this novel methodology. Also in the near future to make this proposed methodology to be adopted in real time environment exploration on the methodology and techniques of encryption approach can also be taken into area of interest. Further incorporating the concepts of efficient load balancing with this

novel data sharing scheme in cloud computing environment would be taken as the future work.

References

[1] G. Pallis, "Cloud Computing: The New Frontier of Internet Computing," IEEE Internet Computing, vol. 14, pp. 70-73, 2010.

[2] X. Xu, "From cloud computing to cloud manufacturing," Robotics and computer-integrated manufacturing, vol. 28, pp. 75-86, 2012.

[3] J. Voas and J. Zhang, "Cloud computing: new wine or just a new bottle?" IT professional, vol. 11, pp. 15-17, 2009.

[4] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in Grid Computing Environments Workshop, 2008.

[5] G. Reese, Cloud application architectures: building applications and infrastructure in the cloud: " O'Reilly Media, Inc.", 2009.

[6] DananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo Security, Privacy and Trust in Cloud Systems, 45 DOI: 10.1007/978-3-642-38586-5_2, © Springer-Verlag Berlin Heidelberg 2014.

[7] Baker, M. Mackay, and M. Randles, "Eternal Cloud Computation Application Development." Developments in Esystems Engineering (DeSE),2011.

[8] F. Fatemi Moghaddam, N. Khanezaei, S. Manavi, M. Eslami, and A. Samar, "UAA: User Authentication Agent for Managing User Identities in Cloud Computing Environments," in IEEE 5th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 2014.

[9] Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing International conference on computer science and electronics, engineering.

[10] Verma R (2012) Confidentiality and privacy issues/ The Law Handbook. Education Law. Oct 2012.

[11] Ruhr (2011) Cloud computing: Gaps in the 'cloud'. News Rx Health Sci. Zunnur hain K, Vrbsky SV (2010) Security attacks and solutions in clouds. CloudCom 2010.

[12] J. Voas and J. Zhang, "Cloud computing: new wine or just a new bottle?" IT professional, vol. 11, pp. 15-17, 2009.

[13] I. Foster, Y. Zhao, I. Raicu, and S. Lu, "Cloud computing and grid computing 360-degree compared," in Grid Computing Environments Workshop, 2008. GCE'08, 2008, pp. 1-10.

[14] G. Reese, Cloud application architectures: building applications and infrastructure in the cloud: " O'Reilly Media, Inc.", 2009.

[15] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, vol. 53, p. 50, 2009.

[16] W. Diffie and M. Hellman. New Directions in Cryptography, IEEE Transactions on Information Theory, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976.

[17] Anoop MS "Elliptic Curve Cryptography An Implementation Guide" IEEE, 2014.

[18] RFC 4492 "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)" 2016.

[19] Ruhr "Cryptographically secure pseudorandom number generator", 2011.

[20] G. Pallis, "Cloud Computing: The New Frontier of Internet Computing," IEEE Internet Computing, vol. 14, pp. 70-73, 2010.

[21] X. Xu, "From cloud computing to cloud manufacturing," Robotics and computer-integrated manufacturing, vol. 28, pp. 75-86, 2012.

[22] J. Voas and J. Zhang, "Cloud computing: new wine or just a new bottle?" IT professional, vol. 11, pp. 15-17, 2009.

[23] Boyang Wang, Baochun Li and Hui Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud",IEEE Transaction, 2015.

[24] Zhao G, Rong C, Li J, Zhang F, Tang Y (2010) Trusted data sharing over untrusted cloud storage providers. IEEE second international conference cloud computing technology and science(CloudCom) 2010.

[25] Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. 13th ACM conference on computer and communications security (CCS '06) 2006.

[26] Wang X, Zhong W (2010) A new identity based proxy re-encryption scheme. International conference biomedical engineering and computer science (ICBECS) 2010.

[27] Yu S,Wang C, Ren K, LouW(2010) Achieving secure, scalable, and fine-grained data access control in cloud computing, INFOCOM, 2010.

[28] Shucheng Yu, Cong Wan, Kui Ren *ASIACCS'10* April 13–16, 2010, Beijing, China. Attribute Based Data Sharing with Attribute Revocation.

[29] Alexandra Boldyreva, Vipul Goyal, Virendra Kumar, Identity-based Encryption with Efficient Revocation, School of Computer Science, College of Computing, Georgia Institute of Technology, 266 Fest Drive, Atlanta.

[30] Autade Dhanshri , S.Y Raut " Review of Public Integrity Auditing and Group User Revocation for Shared Dynamic Cloud Data International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering Vol. 3, Issue 12, December 2015.

[31] MichaelCobb,http://searchsecurity.techtarget.com/tip/Analyzing-the-integrity-of-the-Diffie-Hellman-key-exchange.

[32] Juels, Kaliski. "Pors: proofs of retrievability for large files[C]", Proceedings of CCS 2007. Alexandria, VA,USA, 2007. 584-597

[33] Abhishek Mohta and LK Awasthi, "Robust Data Security for Cloud while using Third Party Auditor" in International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE),Volume No. 2, Issue 2,Feb 2012.

[34] A. J. Menezes, M. Qu, and S. A. Vanstone, "Some key agreement protocols providing implicit authentication," in Proceedings of 2nd Workshop Selected Areas in Cryptography, pp. 22–32, May 1995

[35] R. Cramer and V. Shoup, Design and Analysis of Practical Public-key Encryption ok Schemes Secure against Adaptive Chosen Ciphertext Attack, 2003.

[36] V. Martinez, F, L. Hernandez, Analysis of ECIES and Other Cryptosystem Based on Elliptic Curves,2007.