ISSN:0975-9646

Pooja Dubey et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3795-3798

A Secure & Verifiable Technique for Secure Communication using Elliptic Curve

Pooja Dubey
Computer Science Engineering
Truba Inst. of Engg. and I.T.
Bhopal, India

Prof. Amit Saxena
Computer Science Engineering
Truba Inst. of Engg. and I.T
Bhopal, India

Dr. Manish Manoria
Computer Science Engineering
Truba Inst. of Engg. and I.T
Bhopal, India

Abstract— During the transmission of data from sender prevents from various attacks. Public key encryption is a technique which provides encryption of data using public key. The existing technique implemented for the searching of keywords with public key encryption provides security from password Guessing attacks [1]. But the technique implemented here enables security from various attacks as fine as also provides low computational cost and search time. The proposed methodology implemented here using verifiable encryption using Elliptic Curves provides security with message verification at the receiver.

Keywords—TRNG, Data Sharing, Key Escrow, Proxy Encryption, CP-ABE, OTPK,

I. INTRODUCTION

Page ranking is a concept of providing the best retrieval of web pages according to their ranking. The data from various users in cloud computing can be stored in storage panel according to their identities or keywords [2], [3], [4]. Algorithms for top-k recovery in databases normally try to diminish the numeral of database matter that have to be access before being able to revisit accurate result set of the k best identical substance. The problem to define exact retrieval gets even worse, if top-k queries have to be answered. Besides the difficulties with the instability of the P2P complex, also the heterogeneity of the peers plays a significant part, since each peer only knows its restricted objects and different peers may also feature different scoring or recovery strategies [5].

ENCRYPTION TECHNIQUES

Some amount of data security can be achieved through the encryption of the data.
Some encryption techniques are:
ECIES: The Elliptic Curve Integrated Encryption Scheme (ECIES) is a public-key encryption scheme based on ECC. It is designed to be semantically secure in the presence of an adversary capable of launching chosen-plaintext and chosen-cipher text attacks.
ECC: Elliptical curve cryptography is a community key encryption method based on elliptic curve conjecture that can be used to make faster, less significant and more competent cryptographic keys. ECC produces keys during the properties of the elliptic curve equation as an alternative of the conventional method of creation as the produce of very huge prime numbers. The technology can be used in coincidence with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some examiners, ECC can give way a stage of security with a 164-bit key that other schemes require a 1,024-bit key to accomplish.
AES: It is stand for Advanced Encryption Standard. It is a specification of the electronic data encryption. The Advanced Encryption Standard comprises three block ciphers, AES-128, AES-192 and AES-256. AES as a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. The block-size has a maximum of 56 bits, but the key-size has no theoretical maximum. The cipher uses number of encryption rounds which converts plain text to cipher text. .
DES: It stands for Data encryption standard. It is a widely-used method of data encryption with the help of private or secrete key. DES uses 56-bit key to each 64-bit block of data. It can run in various modes and involves 16 rounds or operations. Although this is considered "strong" encryption, many companies used 'triple DES' that uses three keys in succession.

II. RELATED WORK

Yu, Shucheng et al [6] suggested Attribute based data sharing with attribute revocation. They explore a feasible solution based on novel cryptographic methods. It shows semi-trustable substitute servers that are for eternity accessible for as long as various types of pleased services. The state provided here in this method is based on the semi-trusted servers where the data are shared among various users and the authentication is provided using the attribute policies provided to each user in the network [6].
A. Sahai and B. Waters proposed Fuzzy Identity-Based Encryption. They present two constructions of Fuzzy IBE schemes. This construction can be viewed as an Identity-Based Encryption of a message under several attributes that compose a fuzzy identity. This IBE schemes are both error tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. They prove the security of this scheme under the Selective-ID security model. They first introduced attribute based encryption (ABE) for encrypted access control. In an ABE system, both the user secret key and the ciphertext are associated with a set of attributes. Only if at least a threshold number of attributes overlap between the ciphertext and his secret key, can the user decrypt the ciphertext [7].

Alfin Abraham et al [8] proposed survey of Identity-based encryption with efficient revocation. They propose a new way to mitigate the limitation of IBE with regard to revocation, and improve efficiency of the previous solution. They want to remove interaction form the process of key update, as keeping the PKG online can be a bottleneck, especially if the number of users is very large [8].

Bethencourt et al [9] suggested Ciphertext-Policy Attribute Based Encryption. They provide the first construction of a ciphertext-policy attribute-based encryption (CP-ABE) to address this problem, and give the first construction of such a scheme. In this system, a user's private key will be associated with an arbitrary number of attributes expressed as strings. They created a system for Ciphertext-Policy Attribute Based Encryption. Finally, they provided an implementation of this system, which included several optimization techniques [9].

V. Goyal et al. [10] first introduced the concept of CP-ABE based on ABE. The main idea is to develop a much richer and secure type of attribute-based encryption cryptosystem. In this system each ciphertext is labeled by the encryptor with a set of expressive attributes. Each private key is connected with an access construction that specifies which type of ciphertexts the key can decrypt. They call such an idea a Key-Policy Attribute-Based Encryption (KP-ABE), since the access structure is specified in the private key, while the ciphertexts are simply labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if the attributes associated with a ciphertext satisfy the key's access structure. Their construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) [10].

R. Ostrovsky et al [11] planned Keyword-Based Encryption with Non-Monotonic right of entry Structures. They present a new Keyword-Based Encryption system where confidential keys can represent any access formula over attributes, counting non-monotone ones. In particular, our construction can handle any access structure that can be represented by a Boolean formula. At a high level, the technical novelty in our work lies in finding a way to make a share "available" to the decryptor only if a given attribute is not among the attributes of the ciphertext. In designing this construction several challenges arise from adapting these techniques while preserving the collusion resistance features that are essential for Attribute-Based Encryption systems. They achieved this through a novel application of revocation methods into existing ABE schemes. In addition, the performance of our scheme compares very favorably to that of existing, less-expressive ABE systems. An important goal in ABE systems is to create even more expressive systems [11].

III. Proposed Methodology

The proposed methodology implemented here consists of following phases:

Initialization Phase

During the initial set up of the Elliptic curve we choose an elliptic curve equation. This satisfies the equation,

$$y^2 = ax^3 + bx + c, \qquad where\ 4a^3 + 27b^2 \neq 0$$

Key Generation Phase

Key generation is an important part where we have to generate public key and private key. The sender uses the receiver's public key for the encrypting of the message and the receiver uses his private key to decrypt the message.

Now, we have to select a number as private key 'x' within the range of 'n'.

Now we generate the public key using private key and Base point given as:

y = x * P

x = The random number that we have selected within the range of (1 to n-1). P is the Base point on the curve. 'y' is the public key and 'x' is the private key.

Verifiable Encryption Phase

For encryption, the same elliptic curve parameter is used that was used for key generation and mutual authentication. For the encryption process, we have used the algorithm given by [Elsayed Mohamed et.el in his work "Elliptic Curve encryption with Encrypted Message Authentication and Forward Secrecy"] except they select at random number v from 1.... q-1, while we are using here the identity value to generate random number the key k1 and k2.

k1 = hash(ID.P)
k2 = hash(ID.Qrec)
c = E k2(m)
r = hash (c, k1)
s = ID / (r + Dsen) mod n
R = rP
p=HASH (c||R||s)
Send (c,R,s) to Receiver

Verifiable Decryption Phase

Receiver receives (c,R,s)
c||R||s← (p)
k1 = hash(s(R + Qsen))
=sR+s.Qsen
= ID/(r+Dsen)).rP+(ID/(r+Dsen)).Qsen
= ID.rP/(r+Dsen))+(ID.Qsen/(r+Dsen))
= ID.rP+ID.Qsen/r+Dsen
= ID.rP+ID.Dsen.P/r+Dsen
=ID.P(r+Dsen)/r+Dsen
=ID.P
= k1 =hash(ID.P)
r = hash (c, k1)
k2 = hash(Drec.s(R + Qsen))
=Drec.sR+S.Qsen
=Drec.ID.P
=Drec.P.ID
=Qrec.ID
= k2 =hash(Qrec.ID)
m = Dk2(c)
Accept c only if rP = R

IV. RESULT ANALYSIS

The table shown below is the analysis and comparison of the existing Fuzzy Public Key Encryption Technique and the proposed methodology implemented. Here in the given table the workload and communication costs are denoted by the number of keyword searchable ciphertexts.
n: the total number of keywords searchable ciphertexts stored in the proxy server.
t: the number of keywords searchable ciphertexts satisfied the query of the receiver.

	The workload of the proxy server	The Cost of the Communication	The Workload of the receiver
PEFKS	log(n)	2 log(t)	2 log(t)
Proposed Work	n	2t	2t

Table 1. The performance of the PEFKS & Proposed Work

The table shown below is the analysis and comparison of existing and proposed work. The analysis is done on the basis of number of keywords and computational time to access these keywords.

	Time (ms)	
No. of Keywords	**PEFKS**	**Proposed Work**
10	6.34	2.11
20	10.46	3.42
30	15.28	4.64
40	19.32	7.27
50	21	9.21
60	25.94	10.72
70	30.18	12.53
80	37.42	15.3

Table 2. Comparison of Computational Time

The figure shown below is the analysis and comparison of existing and proposed work. The analysis is done on the basis of number of keywords and computational time to access these keywords.

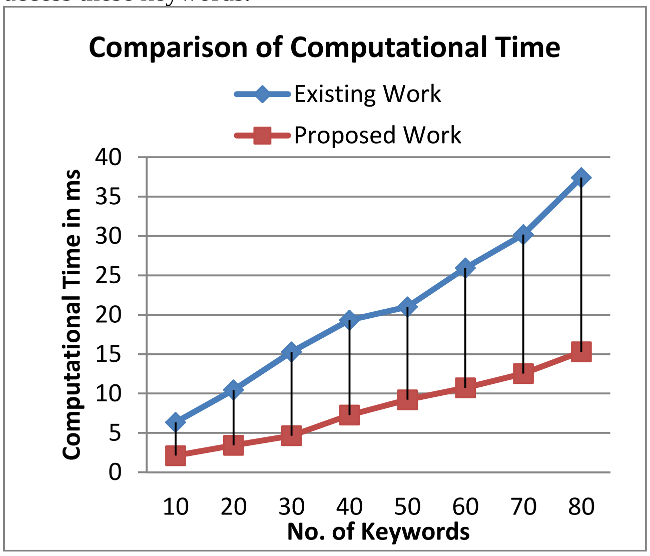

Figure 1. Comparison and analysis of PEFKS & Proposed Work

V. CONCLUSION

The proposed methodology implemented here for the security of data from sender to receiver using Elliptic Curve based key generation and message verification is efficient in terms of computational cost and time as well as it also provides security from various attacks.
The proposed methodology provides security from attacks such as identity disclosure attack, replay attacks and various other attacks.

REFERENCES

[1] Peng Xu and Hai Jin, “Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack”, IEEE 2013.

[2] Yu, Jiadi, Peng Lu, Yanmin Zhu, Guangtao Xue, and Minglu Li. "Towards Secure Multi-Keyword Top-k Retrieval over Encrypted Cloud Data," IEEE transactions on dependable and secure computing, vol. 10, no. 4, pp. 239- 250, July/August 2013.

[3] Pankaj Arora, Rubal Chaudhry Wadhawan and Er. Satinder Pal Ahuja “Cloud Computing Security Issues in Infrastructure as a Service”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, vol. 2, issue 1, Jan. 2012.

[4] Song, Dawn, Elaine Shi, Ian Fischer, and Umesh Shankar. "Cloud data protection for the masses", In IEEE Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] Priya, P. Shanmuga, and R. Sugumar. "Multi Keyword Searching Techniques over Encrypted Cloud Data", International Journal of Science and Research (IJSR), ISSN: 2319-7064, vol. 3, issue 3, pp. 410 -412, March 2014.

[6] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. "Attribute based data sharing with attribute revocation." In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270. ACM, 2010.

[7] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt ’05), pp. 457-473, 2005.

[8] Alfin Abraham, Vinodh Ewards, Harlay Maria Mathew “A Survey on Optimistic Fair Digital Signature Exchange Protocols”, International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397, Vol. 3, No. 2, pp. 821 – 825, Feb 2011.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-PolicyAttribute Based Encryption,” Proceedings IEEE Symposium Security andPrivacy, pp. 321-334, 2007.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,”Proceedings of ACM Conference on Computer and Communication Security, pp. 89-98, 2006.

[11] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-Based Encryptionwith Non-Monotonic Access Structures,” Proceedings ACM Conference Computer and Comm. Security, pp. 195-203, 2007.

[12] Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee et al. "A view of cloud computing." *Communications of the ACM*, vol. 53, no. 4, pp. 50-58, 2010.

[13] Chaudhuri, Surajit, and Luis Gravano. "Evaluating top-k selection queries." *In VLDB, vol.* 99, pp. 397-410. 1999.

[14] Fagin, Ronald, Amnon Lotem, and Moni Naor. "Optimal aggregation algorithms for middleware", *Journal of Computer and System Sciences*, vol. 66, no. 4, pp. 614-656, 2003.

[15] Balke, Wolf-Tilo, and Werner Kießling. "Optimizing multi-feature queries for image databases." *In Proceedings of the International Conference on Very Large Databases*, 2000.

[16] Balke, W-T., Wolfgang Nejdl, Wolf Siberski, and Uwe Thaden. "Progressive distributed top-k retrieval in peer-to-peer networks." *In Proceedings of IEEE 21st International Conference on Data Engineering (ICDE 2005)*, pp. 174-185, 2005.

[17] Wang, Cong, Ning Cao, Jin Li, Kui Ren, and Wenjing Lou. "Secure ranked keyword search over encrypted cloud data." *In Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, pp. 253-262. IEEE, 2010.

[18] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage" *Ieee Transactions On Computers*, VOL. 62, NO. 2, FEBRUARY 2013.

[19] Cao, Ning, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." *Parallel and Distributed Systems, IEEE Transactions on 25*, no. 1 (2014): 222-233, 2014.

[20] Wong, Wai Kit, David Wai-lok Cheung, Ben Kao, and Nikos Mamoulis. "Secure kNN computation on encrypted databases." *In Proceedings of the 2009 ACM SIGMOD International Conference on Management of data*, pp. 139-152, 2009.

[21] Hussain Abo Surrah, "Multi Keyword Retrieval On Secured Cloud" *Asian Journal of Technology & Management Research*, ISSN: 2249 –0892, Vol. 04, Issue – 01, Jan - Jun 2014.

[22] Stephen S. Yau, Fellow And Yin Yin "A Privacy Preserving Repository For Data Integration Across Data Sharing Services", *IEEE Transactions On Services Computing*, Vol. 1, No. 3, July-September 2008.

[23] T. Wood et al., "Black-Box and Gray-Box Strategies for Virtual Machine Migration," *Proceedings of Fourth USENIX Conf. Networked Systems Design and Implementation (NSDI '07)*, pp. 17-17, 2007.

[24] Clark, Christopher, Keir Fraser, Steven Hand, Jacob Gorm Hansen, Eric Jul, Christian Limpach, Ian Pratt, and Andrew Warfield "Live migration of virtual machines", *In Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation*,Vol. 2, pp. 273-286, 2005.

[25] Liu, Haikun, Hai Jin, Cheng-Zhong Xu, and Xiaofei Liao "Performance and energy modeling for live migration of virtual machines", *Cluster computing*, vol. 16, no. 2, pp. 249-264, 2013.

[26] Greveler, Ulrich, Benjamin Justus, and Dennis Loehr. "A Privacy Preserving System for Cloud Computing." *In IEEE 11th International Conference on Computer and Information Technology (CIT- 2011)*, pp. 648-653, 2011.

[27] Mishra, Ranjita, Sanjit Kumar Dash, Debi Prasad Mishra, and Animesh Tripathy. "A privacy preserving repository for securing data across the cloud." *In IEEE 3rd International Conference on Electronics Computer Technology (ICECT-2011)*, vol. 5, pp. 6-10, 2011.

[28] Mishra, Ranjita, Sanjit Kumar Dash, Debi Prasad Mishra, and Animesh Tripathy. "A privacy preserving repository for securing data across the cloud." *In IEEE 3rd International Conference on Electronics Computer Technology (ICECT-2011)*, vol. 5, pp. 6-10, 2011.