IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Secure Data Outsourcing Protocol in Cloud by PRE and ECC with Chaotic Standard Map

Mahendra Kumar Yadav[1], Jashwant Samar[2], Durgesh Wadbude[3]

Research Scholar, Computer Science Engineering, Mittal Institute of Technology, Bhopal (M.P), India[1]

Assistant Professor, Computer Science Engineering, Mittal Institute of Technology, Bhopal (M.P), India[2]

Head of Department, Computer Science Engineering, Mittal Institute of Technology, Bhopal (M.P), India[3]

Abstract: Cloud computing has evolved as one of the most promising technologies as it has the potential to transform the traditional way of computing. It is a technology in which the resources are relying on the Internet and one can use it on pay per use modus operandi. Cloud computing enables the provisioning of these resources on demand in the form of service. Now days everyone uses cloud services for data outsourcing and sharing with. So security of data becomes important issue in cloud computing. Data should be secure and sharing of data should be efficient. To conserve the confidential data of user against untrusted servers, existing solutions generally apply cryptographic methods and reveal data decryption keys only to authentic users. However, doing this process, these solutions obligatory introduce a heavy computation overhead on the data holder for key dispensation and data management. Here we proposed an SDOP (secure data outsourcing protocol) approach for data outsourcing onto the cloud and reduced the heavy computation overhead on the data holder. In our proposed work we used chaotic standard map with proxy re-encryption (paring free unidirectional proxy re-encryption scheme) to provide fast and easy data sharing. By using chaotic standard map we are reducing the calculation overhead, while proxy re-encryption (PRE) makes flexible and easy data outsourcing. On comparing existing EFADS approach with our proposed approach we found that our proposed approach efficient than existing data sharing approach.

Keywords: Cloud computing, Proxy Re-Encryption, EFADS.

1. INTRODUCTION

In cloud computing, data and applications are maintained by central remote server with the help of Internet. Cloud computing allow consumers to use the applications on pay per use methodology on Internet. Cloud computing also allows customers to access their personal files which are stored somewhere else on other computer. Yahoo email, Gmail, or Hotmail etc. are examples of cloud computing. The email management software and the server are fully managed and controlled by the CSP Google, Yahoo etc. and all are providing cloud services on Internet. Because of the interesting features of cloud computing several organizations are using cloud storage for storing their sensitive data. The data can be stored remotely on cloud by the users and can be accessed by other users or clients as and when required. These days one of the prime issue in cloud computing is data security. Data outsourcing onto the cloud can be dangerous because use of Internet by cloud based services which mean less control over the stored data. This paper primarily with the issues related to security and flexibility in cloud, which are nothing but the user's ability to share data securely and efficiently on cloud server. For securing the data on cloud server cryptographic methods are used. Cryptographic methods involve the two processes, first one is encryption process and other one is decryption process. By the use of this cryptographic method, only authorized user who have the decryption key (private key) related to the corresponding data stored on cloud server can access the sensitive information of that particular data outsourced on cloud server by using decryption process with the help of his private key. In above case data holder needs not to decrypt and encrypt the data for other sharers.

Cloud server will alter the cipher text for other data sharer by using re-encryption key. Data holder create re-encryption key by calculating $KGen(PrK_H , PuK_S)$ it gives REK_{gen} where REK_{gen} is re-encryption key, PrK_H is data holder's private key and $PuKey_S$ is data sharer's public key. For optimizing the computational time chaotic standard map is used. Chaos based cryptosystem is much appropriate for cryptography, it is easy to implement on personal computer. So it is fast and have low cost, which make it better than the traditional cryptosystem. In chaos based cryptosystem a key set is created by a chaotic map and encrypt the data bit by bit. To make encrypted data more randomized this chaos based cryptosystem used recurrence of chaotic standard map many times.

Standard map is described by

$$n_{k+1} = (n_k + m_k + j_n + j_m) \text{mod} N,$$

$$m_{k+1} = \left(m_k + j_m + H_C \sin\frac{n_{k+1}}{2\pi}\right) \text{mod} N,$$

where (n_k , m_k) and (n_{k+1} , m_{k+1}) is the original and permutated position of $N \times N$ matrix, (j_n , j_m) random scan couple and H_C is positive integer.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

1.1 Paper Organization

We organized our paper as follows. In section 2, we present the related work and difficulty of achieving optimal time in encryption and decryption. Section 3; describe the preliminaries definitions of PRE and ECC elliptic curve cryptography. In section 4, we proposed our SDOP approach. In section 5, we describe the performance evaluation. In section 6, we give the conclusion of our proposed approach.

2. RELATED WORK

Our proposed SDOP approach fills the area of "proxy re-encryption" and "chaos based cryptosystem". Here we review some research works, which are related to our proposed approach.

PRE Security is a hot topic for research area in cloud computing. Providing security is very essential in cloud computing. Till now many papers are proposed [2, 3, 4, 5, 6 and 7]. The concept of Proxy Re-Encryption is given by Blaze et al. [1] (1998). And the scheme is only bidirectional. Ivan and Dodis [8] introduced simple definitions of the bidirectional and unidirectional PRE, and implemented the functions based on cryptosystem primitives such as IBE (2003). Later on, Ateniese et al. proposed the first unidirectional PRE scheme (2005) and demonstrated some practical applications. In 2007, Canetti and Hohenberger [9] presented the CCA security model for PRE, and demonstrated the first IND-CCA2 secure bidirectional PRE. Tang and Weng solely presented the definition of Type-based PRE Tang, 2008[10] and conditional PRE Weng et al., 2009[11]. There have been numerous papers [1, 12, 13, 14, 15, 16, 17, 18 and 19] on different PRE schemes with different security properties. The proxy re-encryption with anonymity is demonstrated by Ateniese et al. [16]. Later on, Shao et al. [20 and 21] enhanced the idea of anonymity in [16], and presented diverse anonymous PRE scheme. However, all of the existing anonymous PRE schemes need the time-consuming operation–pairings.

However, the proxy in all these scheme provide the facility of transforming all the delegator's original cipher text and enable the decryption rights to delegatee, on the other hand "a proxy can transform the cipher text which is encrypted for one party so that another one can decrypt it by using his own secrete key."

Chaos based cryptosystem recently, designing a chaos based cryptosystem has become a hot topic in the research field. There are many works proposed till now. Lian et al.[22] introduced A block cipher based on the chaotic standard map , which have composition of three parts: a confusion process based on chaotic standard map, a diffusion process, and a key generator. In [23], Fridrich introduced Symmetric Ciphers Based on Two-dimensional Chaotic Maps, and suggested that a chaos-based image encryption scheme should compose of two processes: chaotic confusion and pixel diffusion. Later on, Deep Desai et al. proposed a Chaos-Based System for Image Encryption [24]; it provides encryption and decryption of image of any type, size and shape.

These all above research works are related to our proposed work. Among them the approach proposed by Guiyi Wei et al. [25] (EFADS protocol) are representative. EFADS protocol is a PRE-based data sharing protocol that is the base of our proposed SDOP approach. However, EFADS protocol is not optimized, i.e., It consumes more time in encryption and decryption. Furthermore, the base papers of EFADS protocol the AFGH05 [4] protocols perform time-consuming operation–pairing. YWRL10 [7] is attribute-based encryption (ABE) and slow re-encryption protocol. However, YWRL10 protocol is not flexible. Because the data holder should know the earmarked data consumer's characteristics values before encrypting the shared data (i.e., the pre-decided sharer list is required). The data holder need not to use decryption-then-encryption method can only share the data original generated by the data holder. EFADS protocol provide flexibility of sharing data i.e. data holder can shared data with sharer even the data is not generated but receive from others without disclosing his own private key. At last, their scheme is not efficient as expected due to the requirement of pairings.

3. PRELIMINARIES

Here we give some basic knowledge of Proxy re-encryption and Elliptic curve cryptography required in this paper.

3.1 Proxy Re-Encryption

PRE a unidirectional proxy re-encryption scheme has following probabilistic polynomial time algorithm.

- Setup (p, q, n) = (PuK, PrK). This algorithm outputs a public key and private key.
- KeyG (PrK_H, PuK_s) = REK. The key generation algorithm outputs a re-encryption key REK.
- PRE_Enc (PuK, P) = C. The symmetric encryption algorithm outputs a ciphertext C for plaintext P.
- PRE_ReEnc (K, REK) = K'. The REnc algorithm generates ciphertext K' for key K.
- PRE_Dec (PrK_S, C) = P. The symmetric key decryption algorithm outputs original plaintext P.

Correctness

The correctness property required following conditions.

$$\text{PRE\_Dec [PrK, PRE\_Enc (PuK, P)]} = P,$$
and
$$\text{PRE\_Dec [PrK, PRE\_ReEnc [KeyGen (PrKey}_H, \text{PuKey}_s), C]] = M,$$

Where C is ciphertext for plaintext P under PuK from PRE_Enc.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

3.2 Elliptic Curve Cryptography

ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller [26] in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005 [27].

Elliptic Curve

An elliptic group E_p (a, b) is determined by following computations

$$x^3 + ax + b \bmod p \text{ [for } 0 \leq x < p, \text{ a and b} < p.$$

Where a and b are integers and p is a prime number and must satisfy the following condition.

$$4a^3 + 27b^2 \bmod p \neq 0$$

For each value of x, we are required to find that whether it is in quadratic residue or not. If it is in quadratic residue then elliptic group have two values else the point is not in the E_p (a, b).

Now one need to obtained quadratic residue by computing $x^2 \bmod p$ and $(p-x)^2 \bmod p$ therefore the quadratic residue is Q_p = set of $\frac{p-1}{2}$.

Operation over elliptic

Let the points P = (x_1, y_1) and Q = (x_2, y_2) $\in E_p$ (a, b) and O is point on infinity. The rules over E_p (a, b) are:

1. P + O = O + P = P
2. If P = (x_1, x_2) and Q = (x_1, -y_1) = -P, then P + Q =O
3. If Q ≠ -P, then P + Q = (x_3, y_3)

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$$

where

$$\lambda \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \text{ if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \text{ if } P = Q \end{cases}$$

Elliptic Curve Cryptography

It can be used to encrypt plaintext P, into ciphertext C by encoding plaintext P into a point P_M from the elliptic group E_p (a, b). Then choose a generator point, G $\in E_p$ (a, b), such that smallest value of n for which nG = O is a very large prime number. Then make E_p (a, b) and G public. User select a private key, PrK_H < n and determine the public key $PuK_H = n_A G$. To encrypt the message point P_M for data sharer, data holder choose a random integer k and encrypt the message and get the ciphertext points part P_C using data sharer's public key PuKey.

$$P_C = [kG, (P_M + k\, PuK_S)]$$

At receiver side data sharer got pair of points, P_C , then data sharer calculate the following

$$(P_M + k\, PuK_S) - [PrK_S(kG)] = (P_M + k\, PrK_S G) - [PrK_S(kG)]$$
$$= P_M$$

By computing the above equation data sharer got the plaintext information P_M, corresponding to message M.

4. PROPOSED SCHEME

The approach developed provides a method for fast data encryption and decryption. For chaotic based cryptography we alter our data into a matrix form by using 2D array. Place the text data into tabular form or matrix form so that each array element is a character. And then transform the table or matrix by using chaotic map function, with random couple coordinates and specified key.

We determine random couple(j_n, j_m), by calculating cumulative sum of

$$j_n = \text{rand}\left(\sum(\text{key}(1,1:5))\right),$$
$$j_m = \text{rand}\left(\text{sum}(\text{key}(1,6:10))\right)$$

Now determine the new coordinates for some previous and original coordinates by computing the following

$$x_1 = \text{mod}(u + j_n + j_m + v, N),$$
$$y_1 = \text{mod}\left(v + j_m + 1 * \sin\left(\frac{x_1 * 256}{2\pi}\right), N\right)$$

Where x_1, y_1 are the new generated coordinates,
u, v are the previous and original coordinates,
And N is the size of matrix.

We have modified matrix or encrypted matrix with a specified key. The decryption process is inverse of encryption and equally simple for those who hold the key.

At description level

1. To convert the data into matrix form n_1 = count all character of data or message including space.
2. Check whether n_1 is a perfect square, if not choose a smallest integer value m, which is greater than n_1. m must be a perfect square.
3. Initialize n = squareRoot(m).
4. Create a matrix of n × n order.
5. Put the value of n_1, character by character into n × n matrix.
6. If there are empty cells at the end of the matrix put the space in that empty cell.
7. Apply chaotic standard map method on the matrix and obtained a new modified or encrypted matrix.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

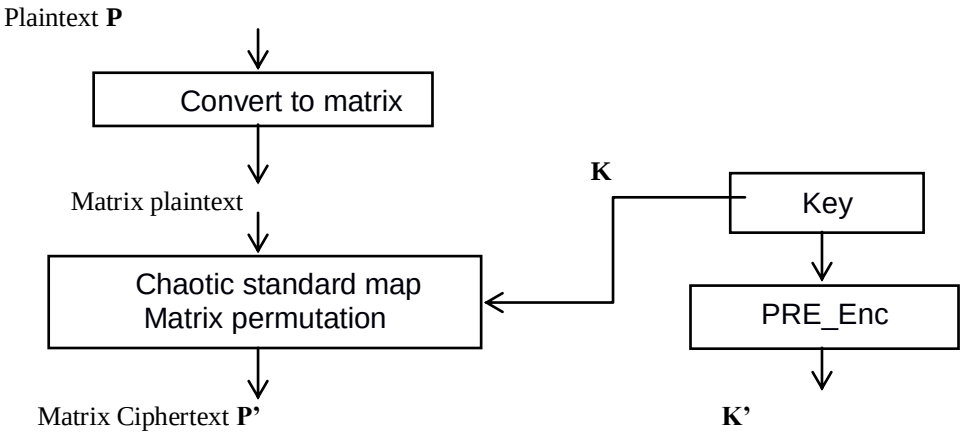

Fig. 1 Encryption process by chaos based cryptosystem.

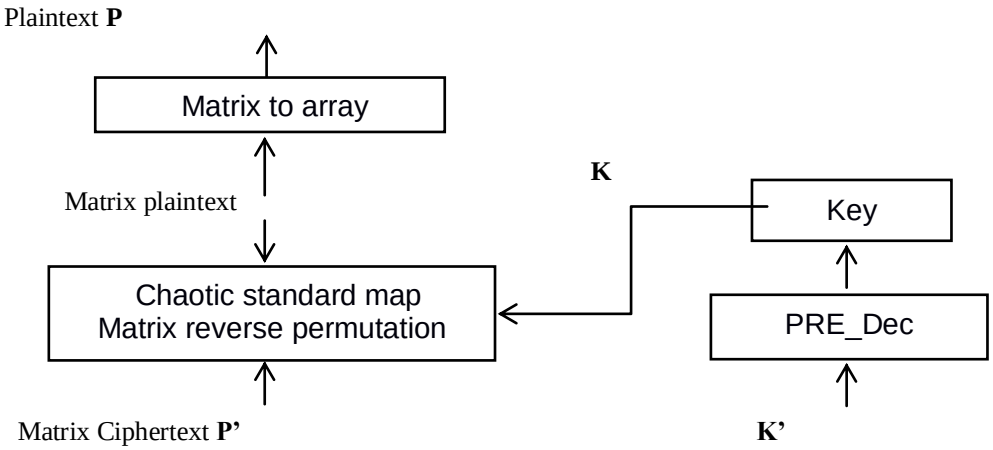

Fig. 2 Decryption process by chaos based cryptosystem.

- Here data holder upload the encrypted file [P', K', I_n] (encrypted by executing P' ← Chaos_Enc (K, P).) and index number related to corresponding encrypted file to the cloud server.
- Then data holder send the re-encryption key (REK, I_n) with index number to cloud.
- If data sharer wants the data from data holder, data sharer ask for data to data holder, then data holder send the index number (I_n) for that particular data.
- Data sharer send the index number (I_n) to the cloud server after that cloud server find the associated data (P', K', I_n) and re-encryption key REK.
- Cloud server transform the encrypted data file (P', K') into (P', K"), and send re-encrypted data file (P', K") to that perticular data sharer.
- At last data sharer determine the key K with his private key PrK_S by executing PRE decryption algorithm, K ← PRE_Dec (PrK_S, K").
- Then obtain the original data content P (plaintext) by executing P ← Chaos_Dec (K, P').

5. PERFORMANCE EVALUATION

A cloud computing system has to short out diverse hurdles security measure, reliability and many more and sometimes unexpected behavior of demands and other various issue which are consider that why experiments cannot be done on the real computing environment if it is done then it will cost to the customer. By using MATLAB 2012b, we implemented our SDOP approach and EFADS protocol (simple with only time complexity) on a personal computer HP equipped with the Intel(R) Core(TM) i5 CPU M350 at frequency of 2.27 GHz that is runs on operating system Windows 8.1. Our proposed algorithm is more efficient and reduces the computation time as compared to EFADS protocol. For respected number of data to encrypt and decrypt, proposed approach give optimal time cost as compared to existing protocol.

In above table we evaluate the performance of individual approach applying on some information message or data message. On the basis of these evaluations we compare our proposed SDOP approach with EFADS protocol and found that computational time cost of our SDOP approach is minimum as compared to EFADS protocol.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Computational time cost of EFADS protocol

Table 1 The experimental results of computational time of EFADS protocol.

S.No.	Plaintext	Ciphertext	Encryption time (in sec)	Decryption time (in sec)
1.	PROXY RE-ENCRYPT	&¨r"XÓ8! • óH» • +	0.003201	0.003369
2.	MITTAL GROUP OF INSTITUTE	°;!a.Ð • Ê0ó\0¬¡H	0.003850	0.004743
3.	RGPV Bhopal	a,DF4J)6v	0.002645	0.002607
4.	Computer Science	H²ÚwÐRgV/ ×ò-	0.003028	0.003120
5.	AICTE New Delhi	Y`&Ò7: ï¤	0.003065	0.002954

Computational time cost of proposed SDOP approach

Table 2 The experimental results of computational time of our proposed SDOP approach.

S.No.	Plaintext	Ciphertext	Encryption time (in sec)	Decryption time (in sec)
1.	PROXY RE-ENCRYPTION	È°íü¸dXQ fî	0.002194	0.002206
2.	MITTAL GROUP OF INSTITUTE	lei4°¥ p6uHS%ætI	0.002872	0.002916
3.	RGPV Bhopal	Ê5	0.001683	0.000963
4.	Computer Science	9ñ$ÅEÙYÕÍÍÉív¡	0.002081	0.002136
5.	AICTE New Delhi	4XB`p>ÝÁ	0.002084	0.002044

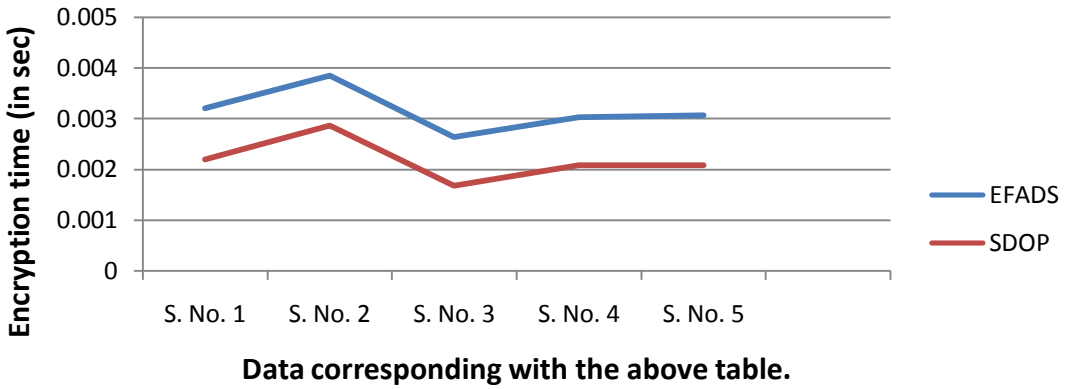

Fig. 1 Computational cost in encryption between our proposed SDOP approach and EFADS protocol.

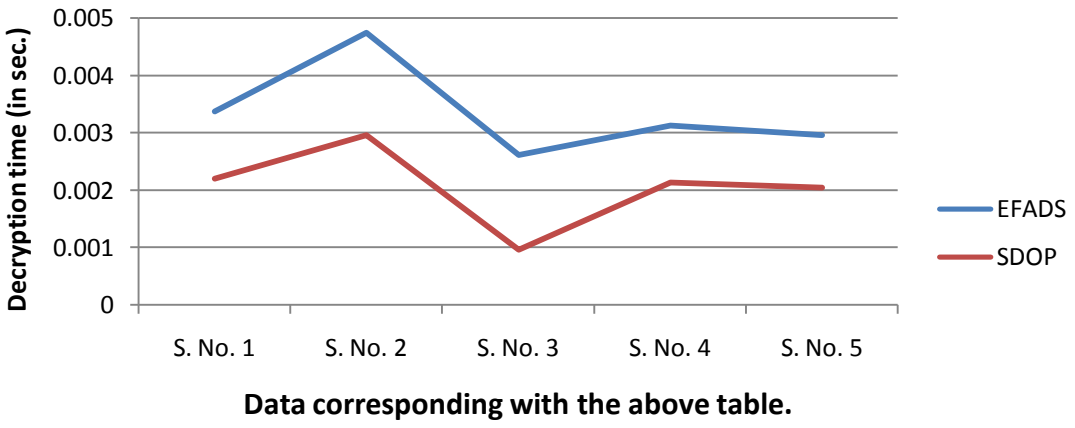

Fig. 2 Computational cost in decryption between our proposed SDOP approach and EFADS protocol.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

6. CONCLUSION

In this paper, we have proposed a secure data outsourcing protocol in cloud by PRE and ECC with chaotic standard map. In our proposed work SDOP approach provide the optimal solution for computational time cost in encryption and decryption of data with the help of chaotic standard map. We also provide the flexibility of sharing data with others without doing a time consuming computation (again encryption and decryption process). The performance evaluation, in which proposed approach is compared with existing approach on computational time cost this technique works well with heterogeneous type of data.

REFERENCES

[1] Blaze, M., Bleumer, G., Strauss, M., 1998. Divertible protocols and atomic proxy cryptography. In: EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144.
[2] Matt Blaze, A cryptographic file system for UNIX, in: Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, Victoria Ashby (Eds.), ACM Conference on Computer and Communications Security, ACM, 1993, pp. 9–16.
[3] Atul Adya, William J. Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, JohnR. Douceur, Jon Howell, Jacob R. Lorch, Marvin Theimer, Roger Wattenho fer, FARSITE: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment, in: Proceedings of the 5th Symposium on Operating Systems Design and Implementation, OSDI, December 9–11,2002, pp. 1–14.
[4] Ateniese, G., Fu, K., Green, M., Hohenberger, S., 2005. Improved proxy re-encryption schemes with applications to secure distributed storage. In: ACM NDSS 2005, pp. 29–43.
[5] Eu-Jin Goh, Hovav Shacham, Nagendra Modadugu, Dan Boneh, Siri US: securing remote untrusted storage, in: NDSS, The Internet Society, 2003.
[6] Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian Wang, Kevin Fu, Plutus: scalable secure file sharing on untrusted storage, in: FAST, USENIX, 2003.
[7] Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing, in: INFOCOM, IEEE Press, 2010, pp. 534–542.
[8] A. -A. Ivan, Y. Dodis, Proxy cryptography revisited, in: NDSS, The Internet Society, 2003.
[9] R. Canetti, S. Hohenberger, Chosen-ciphertext secure proxy re-encryption, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS' 07, ACM, New York, NY, USA, 2007, pp. 185–194.
[10] Tang, Q., 2008. Type-based proxy re-encryption and its construction. In: INDOCRYPT 2008. LNCS, vol. 5365, pp. 130–144.
[11] Weng, J., Deng, R.H., Chu, C., Ding, X., Lai, J., 2009. Conditional proxy re-encryption secure against chosen-ciphertext attack. In: ACM ASIACCS 2009, pp. 322–332.
[12] Susan Hohenberger, Guy N. Rothblum, Abhi Shelat, Vinod Vaikuntanathan, Securely obfuscating re-encryption, in: Salil P. Vadhan (Ed.), TCC, in: Lect. Notes Comput. Sci., vol. 4392, Springer, 2007, pp. 233–252.
[13] Benoît Libert, Damien Vergnaud, Unidirectional chosen-ciphertext secure proxy re-encryption, in: Ronald Cramer (Ed.), PublicKey Cryptography, in: Lect. Notes Comput. Sci., vol. 4939, Springer, 2008, pp. 360–379.
[14] Jun Shao, Zhenfu Cao, Cca-secure proxy re-encryption with out pairings, in: Stanislaw Jarecki, Gene Tsudik (Eds.), PublicKey Cryptography, in: Lect. Notes Comput. Sci., vol. 5443, Springer, 2009, pp.357–376.
[15] Cheng-Kang Chu, Jian Weng, Sherman S. M. Chow, Jianying Zhou, Robert H. Deng, Conditional proxy broad cast re-encryption, in: Colin Boyd, Juan Manuel González Nieto (Eds.), Information Security and Privacy, 14th Australasian Conference, ACISP 2009, Brisbane, Australia, July 1–3, 2009, in: Lect. Notes Comput. Sci., vol. 5594, Springer, 2009, pp. 327–342.
[16] Giuseppe Ateniese, Karyn Benson, Susan Hohenberger, Key-private proxy re-encryption, in: Marc Fischlin (Ed.), Topicsin Cryptology, CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20–24, 2009, in: Lect. Notes Comput. Sci., vol. 5473, Springer, 2009, pp. 279–294.
[17] Jun Shao, Zhenfu Cao, Peng Liu, Cca-secure pre scheme without random oracles, J. Cryptol. 2010 (2010) 112.
[18] Toshihide Matsuda, Ryo Nishimaki, Keisuke Tanaka, Cca proxy re-encryption without bilinear maps in the standard model, in: Phong Q. Nguyen, David Pointcheval (Eds.), Public Key Cryptography, in: Lect. Notes Comput. Sci., vol. 6056, Springer, 2010, pp. 261–278.
[19] Jian Weng, Min-Rong Chen, Yanjiang Yang, Robert H. Deng, Kefei Chen, Feng Bao,Cca-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles, Sci. China, Ser. F53 (3) (2010) 593–606.
[20] Jun Shao, Peng Liu, Guiyi Wei, Yun Ling, Anonymous proxy re-encryption, J. Secur. Commun. Netw. 5 (5) (2012) 439–449.
[21] Jun Shao, Peng Liu, Yuan Zhou, Achieving key privacy without losing CCA security in proxy re-encryption, J. Syst. Softw. 85 (3) (2012) 655–665.
[22] Lian SG, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals 2005; 26(1):117-29.
[23] Fridrich J. Symmetric Ciphers Based on Two-dimensional Chaotic Maps. Int. J.Bifurcat Chaos 1998;8(6):1259-84.
[24] D. Desai, A. Prasad, J. Carsto. Chaos-Based System for Image Encryption, International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4809-4811.
[25] G. Wei, R. Lu, J. Shao. EFADS: Efficient, flexible and anonymous data sharing protocol for cloud computing with proxy re-encryption. Journal of Computer and System Sciences 80 (2014) 1549–1562.
[26] Miller, V. (1985). "Use of elliptic curves in cryptography". CRYPTO. Lecture Notes in Computer Science **85**: 417–426. doi:10.1007/3-540-39799-X_31. ISBN 978-3-540-16463-0.
[27] https://en.wikipedia.org/wiki/Elliptic_curve_cryptography#cite_note-5.