SECURITY IMPLEMENTATION ON CLOUD STORAGE USING NEW PUBLIC KEY ALGORITHM BASED ON BLOCK CIPHER

Prakash Kuppuswamy[*]

Abstract

Cloud computing is a new era of the modern world. It is an emerging paradigm which has become today's hottest research area due to itsability toreduce the costs associated with computing.The main problem associated with cloud computing are data privacy, security and authenticity, the aim of our proposal to give the cloud data storage models and data security in cloud computing system. Here we propose an efficient method for providing data storage security in cloud computing using new public key algorithm based on linear block cipher. This proposed algorithm, which has been proposed and proved other research area such as Data encryption, Ecommerce, Digital signature etc., here, we are implanting the same algorithm on Cloud Computing. In this algorithm some important security services included such as key generation, encryption and decryption that are provided in cloud computing system. The main scope of this paper to solve the security issues in both cloud providers and cloud consumers using new cryptography methods.

Key words: Cloud computing, Data storage, linear block algorithm, Encryption/Decryption.

[*] Lecturer, Computer Engineering & Networks Department, Jazan University, Jazan, KSA.

I. Introduction

Computing facilities and applications will rapidly increase and delivered as a service over the Internet. Cloud computing provides Internet-based services and storage for users in all markets including financial, healthcare, education and government[2].Cloud Computing is the key driving force in many small,medium and large sized companies and as many cloud usersseek the services of cloud computing, the major concern is thesecurity of their data in the cloud. Securing data is always ofvital importance and because of the critical nature of cloudcomputing and the large amounts of complex data it carries,the need is even more important. Hence forth, concernsregarding data privacy and security are proving to be a barrierto the broader uptake of cloud computing services [1].

Just a few years ago, people used disk to store their documents. In recent times, many people moved to memory sticks. Cloud computing refers to the ability to access and manipulate the information which was stored on remote servers, using any Internet-enabled platform. There are four types of cloud models listed by NIST (2009): private cloud, public cloud, hybrid cloudand community cloud [2].

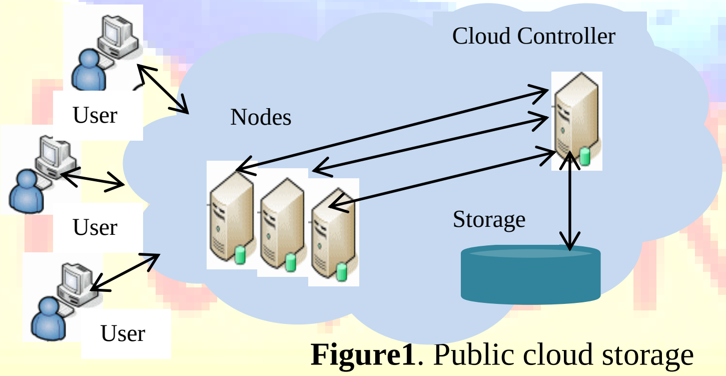


Figure1. Public cloud storage

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet. Cloud computing shared resources areprovided like electricity distributed on the electricity grid. There are many advantages using by the Cloud computing such as Reduced Cost, Increased Storage, Organizations can store more data than on private Computer systems, Highly Automated,Flexibility, More Mobility [3].Also, there are five types of issues raise while discussing security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues
5. Trust Issues [3]

II. Literature Review

ParsiKalpana, SudhaSingaraju (2012) discussed about cloud security, the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the Cloud user. To ensure the security of data, we proposed a method by implementing RSA algorithm [1].

K. Sunitha, S.K Prashanth (2013) proposed research paper, that aims to give the cloud data storage models and data security in cloud computing system. Here we propose an efficient method for providing data storage security in cloud computing using RSA algorithm. In this algorithm some important security services included such as key generation, encryption and decryption that are provided in cloud computing system[2].

P. Subhasri, Padmapriya (2013)discussedproblem associated with cloud computing is data privacy, security, data stealing, etc. In this paper we have proposed the new level of data security solution using the Reverse Caesar cipher algorithm with encryption using ASCII full 256 characters, compared between other encryption methods , our new encryption algorithm is very secured level. The main scope of this paper to solve the security issues in both cloud providers and cloud consumers using cryptography encryption methods. It is complicated to understand the cipher text compared with the other methods[3].

SanjoliSingla&Jasmeet Singh (2013)discussed Cloud being the most vulnerable next generation architecture consist of two major design elements i.e. the Cloud Service Provider(CSP) and the

Client. Even though the cloud computing is promising and efficient, there are many challenges for data privacy and security. This paper explores the security of data at rest as well as security of data while moving[4].

Sachindra K. Chavan, M. L. Bangare (2013)discussed a CRM (Customer Relational Management) system services is represented in this paper using RC5 algorithm. In the proposed system the party that uses cloud storage services must encrypt data before sending it to cloud while the service provider who is responsible for encryption/decryption of the user's data and then must delete data once encryption/decryption process is completed. In this paper the use of CRM services which demonstrates how the parties involved in secure storage and retrieval when data is saved to the cloud[5]

PrakashKuppuswamy, Chandrasekar (2011)proposed new algorithm, which is based on linear block cipher. Encryption as cipher text use invertible square matrix, blocking the message according to the selected square matrix i.e if the square matrix is 3 x 3 make the message or plain text 3 blocks, and select 'e' as any natural number and multiply with selected matrix and message, use modulation 37, then the remainder is our cipher text or encrypted message. This factor is then transmitted. The concept of this new algorithm is based on modular 37 (alphabets an numerals) whereas existing algorithms are based only on modular 26 (only alphabets)[6].

.

III. Proposed Work

Our proposed method similar type of RSA algorithm based on block cipher.Here, we introduce our new algorithm is public key algorithm. The major advantage of asymmetric cryptography is to use two different keys, one Public (open) key and one Private (secret) key. By securing the data, we arenot allowing unauthorized access to it.User data is encrypted first and then it is stored in theCloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user anddelivers the data.

Our new block cipher algorithm consists of Public-Key and Private-Key. Inour Cloud environment, Pubic-Key is known to all, whereasPrivate-Key is known only to the user who originally owns thedata. Thus, encryption is done by theCloud service providerand decryption is done by the Cloud user or consumer. Oncehe data is encrypted with the Public-Key, it can be decryptedwith the corresponding Private-Key only. Our proposed algorithm comprises 3 parts were as follows:-

1. Key Generation
2. Encryption
3. Decryption

3.1.*Key Generation*

Selecting the r x r matrix is the key component of the new digital signature algorithm. Our algorithm based on the modulo 37. So therefore we can keep always public key as 37.

Step 1: Assign the value of n = 37
Step 2: Select invertible matrix i.e „k
Step 3: k should be giving the result of (k*k^{-1}) mod 37 = 1
Step 4: Select any integer value and multiply with "k" i.e., called "d" private key
Step 5: Find inverse of the integer value and multiply with inverse matrix i.e called "e" another public key.Now announce "n" and "e" as public key and "d"& k^{-1} as a private key.

3.2. Encryption technique

Encryption is the process of converting original plain textdata into cipher text (data).
steps:

i. Cloud service provider should give or transmit the Public-Key (n=37, e) to the user who want to store the data with him or her.
ii. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
iii. Data is encrypted and the resultant cipher text (data) C = (k *P)mod n.
iv. This cipher text or encrypted data is now stored with the Cloud service provider.

3.3. Decryption Technique

Receiving the plaintext from cipher text using the key is called decryption or deciphering or decoding. Our New linear block cipher decryption sequences were as follows:-

Steps:

i. The cloud user requests the Cloud service provider for the data.

ii. Cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, C.

iii. The Cloud user then decrypts the data by computing P = $(k^{-1}* C)$ mod n.

iv. Once m is obtained, the user can get back the original databy reversing the padding scheme.

IV. Implementation

In order to provide quick and simple secured cloud computing encryption/decryption, the bits size of the secret key has to be chosen effectively. For encrypting small amount of data, there should not be any overhead to the encrypting system as well as there should not be any compromise on the security level.

Consider here product or message or plain text is ‘INDIA’ i.e equivalent to 9, 14, 4, 9, 1 as per the alphabetical order.

4.1 Key generation process

Now we are chosen k = $\begin{pmatrix} 2 & 1 \\ 4 & 5 \end{pmatrix}$

Finding the inverse of k or k^{-1} or secret key

C11 $[-1]^{1+1}$ x [5] = [-1]2 x [4] = 5
C12 $[-1]^{1+2}$ x [4] = [-1]3 x [3] = -4
C21 $[-1]^{2+1}$ x [1] = [-1]3 x [1] = -1
C22 $[-1]^{2+2}$ x [2] = [-1]4 x [2] = 2

$$\begin{pmatrix} 5 & -1 \\ -4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 7 & 6 \\ 24 & 25 \end{pmatrix}$$

IJMRA

Inverse of k= * -6 mod 37 =

4.2 Encryption process

Now we are calculating message with selected key using encryption algorithm
Customer Token = (k * p) mod 37

$$\begin{pmatrix} 2 & 1 \\ 4 & 5 \end{pmatrix} \begin{pmatrix} 9 \\ 14 \end{pmatrix} * \text{mod37} = \begin{pmatrix} 32 \\ 106 \end{pmatrix} \text{mod } 37 = \begin{pmatrix} 32 \\ 32 \end{pmatrix}$$

Therefore message (9,14,4,9,1,37) will becomes (32,32,17,24,2,4)

4.3 Decryption process

Now we are calculating message with selected key using encryption algorithm
Customer Token = $(k^{-1}$ * c) mod 37

$$\begin{pmatrix} 7* & 6 \\ 24 & 25 \end{pmatrix} \begin{pmatrix} 32 \\ 32 \end{pmatrix} \text{mod37} = \begin{pmatrix} 9 \\ 14 \end{pmatrix}$$

Therefore message (32,32,17,24,2,4) will becomes (9,14,4,9,1,37)

V. Result Discussion

IJMRA

Encryption technique is very authoritative and straight forward. In this algorithm, we can make any number of square matrix according to block of text. The algorithm based on the “r x r” square matrix. Therefore we can select square matrix with any variables. If comparing to other algorithm, The RSA algorithm calculates each and every text variable for encryption. The ElGammal algorithm produces two different cipher texts for single encryption. The Rabin method produces 4 cipher texts for single encryption. In our New algorithm we can make set of blocks in single encryption. Table 8 clearly indicates about encryption methods of various algorithms.

The decryption of new algorithm is complex without the private key. All the plain text is decryption using inverse matrix as a key, Therefore it is providing secure from the unauthorized entities and susceptible. Moreover we are sending secret key through secured channel through key distribution centre or valid entity. If comparing to other algorithm, The RSA algorithm decrypting the cipher text one by one. The ElGammal algorithm receives the two cipher text and calculating decryption once. The Rabin method receives the 4 cipher texts and decryption using 4 steps to find a feasible solution. In this new proposed algorithm we receive set of blocks variable and decryption also using single steps. The following table clearly indicates about encryption decryption methods of various algorithms.

Table 1. Algorithm Comparison

Algorithm	**No. of Text**	**Encryption cycle**	**Decryption cycle**
RSA	100	100	100
ElGammal	100	200	100
Rabin	100	400	100
Proposed (Nlbc)	100	25 (4 block) 50 (2 block)	25 (4 block) 50 (2 block)

VI. Conclusion

Data security has become the most important issue for cloud computing security. Though many solutions have been proposed, many of them only consider 26 alphabets only. It depends upon the way Cloud Service Provider (CSP) allows its client to get registered with his cloud network. In our survey we analyze how security is provided to the data at rest i.e. encryption is done by the cloud service provider.The hill cipher or linear block cipher openness to cryptanalysis has rendered itunusable in practice for the public key algorithm. It still serves an important academic role in both cryptology and linear mathematics. In our new linear block cipher public algorithm, that raises several interesting questions such as key generation method, key distribution method, security concern. Our proposed methods capture the new idea of general usage in commercial sector. Theoretical challenge is to study proofs of security for key refreshing in the standard model.

References

1) ParsiKalpana, SudhaSingaraju, “Data Security in Cloud Computing using RSA Algorithm”, International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol. 1, Issue 4, September 2012.

2) K. Sunitha, S.K Prashanth, “Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm”, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 12, Issue 5, PP 62-64, Aug, 2013.

3) P. Subhasri, Padmapriya, “Implementation of Reverse Caesar Cipher Algorithm for Cloud Computing”, International Journal for Advance Research in Engineering and Technology, Vol. 1, Issue VI, ISSN 2320-6802, July 2013.

4) SanjoliSingla&Jasmeet Singh, “Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm”, Global Journal of Computer Science and Technology Software & Data Engineering Volume 13 Issue 5 Version 1.0 Year 2013.

5) Sachindra K. Chavan, M. L. Bangare, “Secure CRM Cloud Service using RC5 Algorithm”, International Journal of Computer Trends and Technology- volume4, Issue3- 2013.

6) PrakashKuppuswamy, C.Chandrasekar, Enrichment of Security through Cryptographic Public key Algorithm based on Block Cipher, ISSN : 0976-5166 Vol. 2 No. 3 Jun-Jul 2011.

7) M. Baker, R. Buyya, and D. Laforenza, “Grids and grid technologies for wide-area distributed computing,” International Journal of Software:Practice and Experience, vol.32, pp. 1437-1466, 2002.

8) B. R. Kandukuri, V, R. Paturi and A. Rakshit, “Cloud security issues,”in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

9) R. Sterritt, “Autonomic computing,” Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.

10) R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.

11) L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.

12) R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems”, Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.

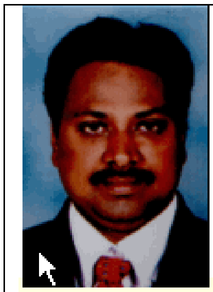
13) V. Miller, “Uses of elliptic curves in cryptography,” Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, pp. 417-426, 1986.

14) Norman D. Jorstad, Landgrave T. Smith, Jr., “Cryptographic Algorithm Metrics”, Institute for Defense Analyses Science and Technology Division, Jan 1997.

15) Harsh Kumar Verma, Ravindra Kumar Singh, “Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms” , in International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012.

IJMRA

Author's Detail:

	**PrakashKuppuswamy**, Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar-Doctorate Degree yet to be awarded by 'Dravidian University'. He has published 20 International Research journals/Technical papers and participated in many international conferences in Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms.

IJMRA