Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 6, Issue, 03, pp.5734-5737, March, 2014

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

ENHANCED SECURITY FOR CLOUD STORAGE USING LINEAR BLOCK CIPHER ALGORITHM

[1]Saleh Mohammed Al-Turki and PrakashKuppuswamy

[1]College of Computer Sciences and Information System, Jazan University, KSA
[2] Computer Engineering and Networks Department, Jazan University, KSA

ARTICLE INFO

Article History:
Received 06th December, 2013
Received in revised form
15th January, 2014
Accepted 18th February, 2014
Published online 25th March, 2014

Key words:
Cloud computing,
Security, Encryptionalgorithms,
Decryption algorithms,
Block cipher, Hill cipher,
Symmetric key.

ABSTRACT

Cloud Computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. Cloud computing, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud Computing stores 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. The main scope of this paper to solve the security issues in both cloud providers and cloud consumers using existing hill cipher symmetric key algorithm with some implementation on modulo function.

INTRODUCTION

Today world cloud computing is very vital role play in technology fields, as we say that cloud computing is a technology that expends the internet and central remote servers holding data and applications. This cloud computing technology allows customers for much more efficient computing and accessing data & files by centralizing data storage and processing. Cloud computing is new demands and delivery model for IT services in present worldwide, is also modern Information System design; this is very useful for users those not understanding the operating systems, client-server architectures, and browsers. Cloud computing has provided users from hardware requirements and reducing overall client side demands and complexity (Tauseef Ahmad *et al*., 2013).Cloud computing is a broad solution that delivers IT as a service. Cloud is an internet based technology uses the internet & central remote servers to support data and applications. It permits consumers and businesses putting to use without installation and approach their personal files at any computer with internet access. Before cloud computing, websites and server based applications were executed on a specific system. The cloud computing flexibility is a function of the allocation of resources on authority's request. And the cloud computing provides the act of uniting.

Corresponding author: Prakash Kuppuswamy
Computer Engineering and Networks Department, Jazan University, KSA.

A cloud is a pattern of parallel and distributed system be composed of a collection of interconnected and virtualized computers that are dynamically stipulation and presented as one or more unite computing resources established on service level agreements found amongst negotiation between the service supplier and consumer (Subhasri and Padmapriya, 2013). There are many types of cloud storage providing data security such as Public cloud, Private cloud, Hybrid cloud and Community cloud.

Public Cloud: The cloud computing resource is shared exterior, someone can use it and a few payments maybe count. Public organizations assist in supplying the infrastructure to carryout the public cloud.

Private Cloud: private cloud resource is boundary to a collection of people, like a staff of a company. Infrastructure of private cloud is perfectly controlled and corporate data are completely supported by the organization itself.

Hybrid Cloud: This is the combination of public as well as private cloud. It can also be explained as multiple cloud systems that are related in a way that permits programs and data to be moved comfortably from one system to another.

Community Cloud: The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause (mostly security). Infrastructure is to be shared by several organizations within specific community with common

security, compliance objectives. It is managed by third party or managed internally. Its cost is lesser then public cloud but more than private cloud (EmanM.Mohamed *et al*., 2013).For securing the cloud storage various algorithm techniques are using. We are implementing Hill cipher here, It was invented by L.S. Hill (1929). It is a famous polygram and a classical symmetric cipher based on matrix transformation but it succumbs to the known-plaintext attack (Stinson, 2006). Although its vulnerability to cryptanalysis has rendered it unusable in practice, it still serves an important pedagogical role in both cryptology and linear algebra. The Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for encryption and decryption, and its high speed and high throughput (Ismail*et al*., 2006). Some of the Key features of Cloud computing storage security as follows:-

- Architecture
- Identity and Access
- Availability
- Incident response
- Governance
- Compliance
- Trust

BACKGROUND REVIEW

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) (PrakashKuppuswamy *et al*., 2011).

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 (Sunitha and Prashanth, 2013).

P. Subhasri, Padmapriya (2013) discussed problem 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 (Subhasri and Padmapriya, 2013).

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 (SanjoliSingla and Jasmeet Singh, 2013).

Sachindra K. Chavan, M. L. Bangare (2013) discussed a Customer Relational Management system a service 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 (Sachindra *et al*., 2013).

PROPOSED ALGORITHM

The algorithm of encryption and decryption of the technique is to use text and numbers during implementation of the message algorithm. Here, we introduce new modified hill cipher symmetric key algorithm. The major advantage of symmetric cryptography is to use same keys for the encryption and decryption. It can be send through secured channel to the receiver.

Existing hill cipher algorithm

1. Find an n x n matrix E that is invertible modulo 26. This is actually the encryption key.
2. Take the message that is to be sent (the plaintext)
3. Convert each character to a number between 0 and 25. The usual way to do this isA = 0, B = 1.., Z = 25.
4. Divide this string of numbers up into blocks of size n. Note that if E is an n x nmatrix then the block size is n. Another note, if the message does not break evenly into blocks of size n we pad the ending of the message with characters, this can be done at random.
5. Write each block as a column vector of size n.
6. Take each of the vectors and multiply them by the encryption matrix E.
7. Take the vectors w1; w2; : : : ; wt, write the entries of the vectors in order, convert thenumbers back to characters and you have your ciphertext.

Cipher Text =(K * Plain text)mod 26
Plain text = (K^{-1} * Cipher text) mod 26

Proposed modified hill cipher algorithm

1. Find an n x n matrix E that is invertible modulo 26. This is actually the encryption key.
2. Take the message that is to be sent (the plaintext)

3. Convert each character to a number between 0 and 25. The usual way to do this is A = 1, B = 2, C = 3……. Z = 26 and 0=27, 1=28, 2=29……9=36
4. Divide this string of numbers up into blocks of size n.
5. Write each block as a column vector of size n.
6. Take each of the vectors and multiply them by the encryption matrix E.
7. Take the vectors w1; w2; : : : ; wt , write the entries of the vectors in order, convert the numbers back to characters and you have your cipher text.

Cipher Text =(K * Plain text)mod 37
Plain text = (K^{-1} * Cipher text) mod 37

IMPLEMENTATION STRUCTURE

The typical setting of a Cloud computing storage system will be wide spread and include individual sub-systems to derive vital data from some specific User/Agent authorization. Following picture shows the block diagram proposed model of cloud storage system, it consists of two phases, namely Key Management Services and Authentication phase accessed by the Agent/User and it is controlled by the Cloud Administrator.The key management service is responsible and providing encryption keys based on requisition from the Agent/User.In Agent/User phase avail the key from the Key Management and secure the data with the help of key from the Key Management Service. The Cloud Administrator is responsible for the transaction between Key Management Service and User.

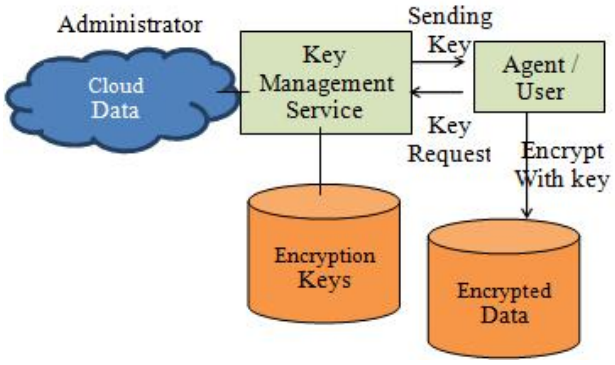

Fig.1. Proposed cloud storage structure

The cryptography presented in this paper could be augmented with a payment mechanism: a commercial entity could accept payment from Administrator and exchange for providing a common public scheme of using natural numbers. Here we consider a cloud message including the numbers “Cloud 2014” to be sent. The sample Cloud message is “Cloud 2014” (including alphabets and numbers). In this paper each alphabet and number is replaced by natural numbers 1to 36(26 alphabets +10 numerals (0-9)). So the encrypted characters are shown in the following table.

Table 1. Encrypting cloud data with key

Block No.	Cloud Message	Message (3)			Integer Value
1		C	L	O	3,12,15
2	CLOUD	U	D	2	21,4,29
3	2014	0	1	4	27,28,31

select ‘k’ =

$$\begin{pmatrix}1&2&1\\4&5&6\\7&8&9\end{pmatrix}\bullet\begin{pmatrix}3\\12\\15\end{pmatrix}=\begin{pmatrix}42\\162\\252\end{pmatrix}\ \text{mod } 37=\begin{pmatrix}5\\14\\30\end{pmatrix}$$

Similarly Block 2 and 3 value (21,19,33) and (3, 27, 26)
Equivalent message for the CLOUD2014 is EN3US6C0Z

Table 2. Message Decryption

BlockNo.	Cloud Message	Message (3)			IntegerValue
1		E	N	3	5, 14, 30
2	EN3US6C0Z	U	S	6	21, 19, 33
3		C	0	Z	3, 27, 26

$$\begin{pmatrix}18&23&32\\1&25&12\\18&1&18\end{pmatrix}\bullet\begin{pmatrix}5\\14\\30\end{pmatrix}=\begin{pmatrix}1372\\715\\644\end{pmatrix}\ \text{mod } 37=\begin{pmatrix}3\\12\\15\end{pmatrix}$$

Similarly Block 2 and 3 value (21,4,29) and (27, 28, 31)
Equivalent message for the EN3US6C0Z is CLOUD2014

RESULT AND DISCUSSIONS

For our experiment, we use a laptop IV 2.4 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 100 K byte to 1000 K Byte. Several performance metrics are collected: encryption time, CPU process time, and CPU clock cycles and battery power. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. The decryption is complex without the private key. All the plain text are decrypted using inverse matrix as a key. Therefore it provides security from the unauthorized entities and susceptible. Data Encryption Standard, was the first encryption standard faced many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher. 3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. RC6 was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Proposed algorithm is 26^{n2} matrices of dimension n × n. additionally it seems to be prudent to avoid too many zeroes in the key matrix, since they reduce diffusion. The net effect is that the effective keyspace of a basic Hill cipher is about 114 bits. Of course, key search is not the most efficient known attack.

Table 3. Encryption performance

No.ofKbytes	DES	3DES	RC6	HillCipher
	Kb/M.Seconds			
100	49	81	60	40
300	82	167	109	70
900	240	300	162	150
Average	371	548	331	260

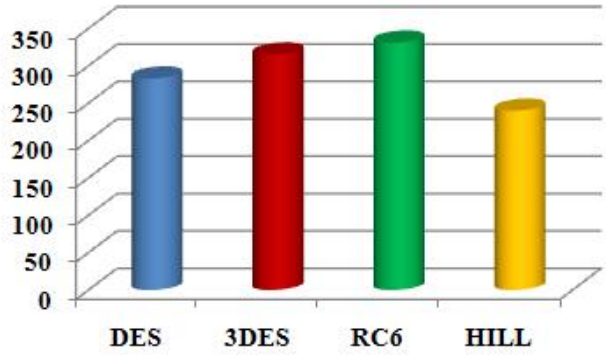

Fig. 2. Encryption execution time (1300 Kb/M.Seconds)

Table 4. Decryption performance

No.ofKbytes	DES	3DES	RC6	Hill Cipher
		Kb/M.Seconds		
100	57	57	58	35
300	74	87	100	65
900	152	171	150	140
Average	283	315	308	240

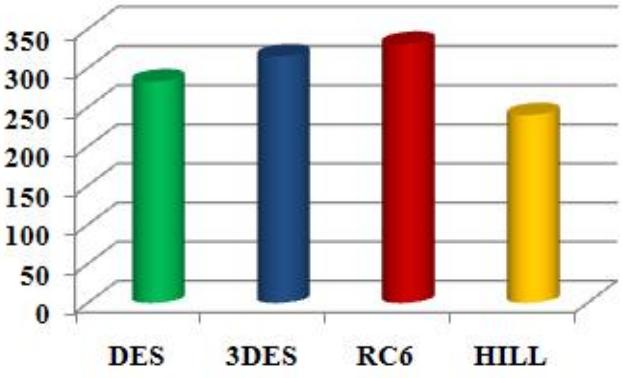

Fig. 3. Decryption execution time (1300 Kb/M.Seconds)

Conclusion

The reason for selecting linear block cipher for our cloud storage security; The linear algebra will not produce same kind of result for the repeated text variable. Also, we can construct 2 block, 3 block square matrix variable each and every time, which will secure our algorithm more. Another advantage for the linear block cipher, we can use negative variable for selecting the square matrix. Another innovative idea for our New algorithm; we are extending characters upto 37 letters. Most of the algorithms are working based on the 26 alphabets, especially hill cipher or linear block cipher. There are a few highlight points about our experimental setup, First, A comparison is conducted between the results of theselected different encryption and decryption Schemes. Second,A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm. Third, A study is performed on the effect of changing data types such as text and numbers.Finally, A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

REFERENCES

Tauseef Ahmad, Mohammad AmanulHaque, Khaled Al-Nafjan, Asrar Ahmad Ansari, Development of Cloud Computing and Security Issues, Information and Knowledge Management, www.iiste.org, ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol.3, No.1, 2013.

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.

Sunitha, K., 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, August, 2013.

Subhasri, P., 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.

Eman M. Mohamed, Hatem S. Abdelkader, Sherif El-Etriby, "Data Security Model for Cloud Computing", The Twelfth International Conference on Networks: ICN 2013.

Hill, L.S. "Cryptography in an Algebraic Alphabet," American Mathematical Monthly, Vol.36, No.6, pp.306-312, 1929.

Stinson, D.R. "Cryptography Theory and Practice," 3rd edition, Chapman & Hall/CRC, pp.13-37, 2006.

Ismail, I.A., M. Amin, and H. Diab, "How to repair the Hill cipher," *Journal of Zhejiang University-Science* A, Vol.7, No.12, pp.2022-2030, Dec. 2006.

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.

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

Vaquero,L. M., 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.

Rivest, R., 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.

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

Norman D. Jorstad, Landgrave T. Smith, Jr., "Cryptographic Algorithm Metrics", *Institute for Defense Analyses Science and Technology Division*, Jan 1997.

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

****