Journal of Theoretical and Applied Information Technology
10th May 2014. Vol. 63 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

KEYLESS CRYPTOGRAPHY IN GRID COMPUTING USING CYCLIC SHIFT TRANSPOSITION ALGORITHM

[1]S. GOMATHI, [2]DR.D.MANIMEGALAI
[1]Assistant Professor,FXEC, Tirunelveli, Tamilnadu, India
[2]Prof & Head, ITDept.,NEC,Kovilpatti, Tamilnadu,India

E-mail: [1]gomathi103@yahoo.in

ABSTRACT

Grid computing involves in the process of forming dynamic virtual organizations and associated resources in which the security is an important factor.Grid computing, is a distributed computing model in which new kind of systems are combined to form a heterogeneous computational resources such as computers, storage space, sensors, and experimental data. The grid can seamlessly, transparently and dynamically supply the computing and data resources when a user wants to request them. In recent years, security issues has become an important concern for grid computing. A strong mutually encrypted and decrypted methodology is needed for user and to prevent the grid resources from being illegally visited. Many cryptographic schemes have been proposed in recent periods for solving the security issues.However, most of them are not ideal for the grid computing technologydue to its computational overhead and the standard of encryption. In this paper, we proposed a keyless Cyclic Shift Transposition Algorithm(CSTA) which uses a combination of shifting and transposition without public or private key to secure the data in the grid computing system. Experimental results shows that the proposed algorithm prevents not only known attacks but also maintains the integrity of data.

Keywords: *Grid Computing, Authentication, Encryption, Decryption, Cipher Text, CSTA*.

1. INTRODUCTION

A Grid is a type of parallel and distributed system that enables the sharing, selection, and aggregation of geographically distributed autonomous and heterogeneous resources dynamically at runtime, depending on their availability, capability, performance, cost, and users' quality-of-service requirements [3]. A grid is also an organized , secured environment managed and controlled by administrators .Compared with cluster computing which only deals with parallelism, the grid is characterized with high heterogeneity, large- scale parallelism .Thus, it can offer advanced services on top of very large amount of distributed data [9].

The main objective of grid computing is to provide secure grid service to the resources .For the legal users the security issue becomes an important concern of grid computing. The nodes are dynamically connected and disconnected in the grid environment. The user authentication is the important factor for security [4]. Authentication deals with verification of the identity of an entity within a network. An entity may be a user, a resource or a service provided as part of the Grid.

To prevent the illegal users from visiting the grid resources, it should be guaranteed that strong mutual authentication needed for users and server. Anyway most of them are not are not ideal for grid computing. Mostly they are based on smartcard and do not provide the strong authentication [1].

Cryptography is the practice and studyof techniques for secure communication in the presence of third parties. More generally, it is about constructing and analysingprotocols that overcome the influence of adversaries and which are related to various aspects in information security [12] such as data confidentiality, data integrity, and authentication. Cryptology-related technology has raised a number of legal issues. Modern time cryptography refers encryption, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called cipher text). Decryption is the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

reverse, in other words, moving from the unintelligible cipher text back to plaintext.

A cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a key. This secret key parameter is ideally known only by the communicants for a specific message exchange context. A "cryptosystem" is an ordered list of elements of finite possible plaintexts, finite possible cipher texts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless. Ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters. Simple versions of cipher have never offered much confidentiality from enterprising opponents. An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter to some fixed number of positions further down the alphabet.

2. RELATED WORKS

One of the services provided by grid is to offer security. But on the other hand it results in performance degradation due to overhead in offering desired level of security.

In the year 1976, Diffie and Hellmann proposed a new kind of cryptosystem which has encryption and decryption keys which are different from each other. Diffie–Hellman key exchange (D–H) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography [sec eng]. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric keycipher.

Hellman suggested the algorithm called as Diffie–Hellman–Merkle key exchange It is also known as public-key cryptography (Hellman, 2002). Although Diffie–Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite). Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network.

Chang et al [8] worked out an algorithm by name International Data Encryption Algorithm IDEA) in the year 1990. A 128 bit key was used for encryption that needs both software and hardware units to implement. In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption [5], and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.

In 2004, Chang et al. proposed a secure, efficient, and practical password authentication scheme without using the server public key. They presented more efficient password authentication scheme that does not use the server public key and that can simply update user passwords without additional message transmission [8].

Guilin system is based on hash function, and mobile users only do symmetric encryption and decryption. In their system, encryption takes only one round of messages exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network. [13]

AnithaKumari.K proposed a trigon based authentication and authorization scheme for grid computing. For distribution of channels the author used MD5 algorithm which is used to reduce computational load using GLOBUS as middleware. This Trigon based authentication [7] and authorization is used to maintain strong

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

security by splitting the password and storing in two files [2].

Fei et al presented a key-exposure free online/offline signcryption scheme .Their scheme proved indistinguishable against adaptive chosen-cipher text attacks (IND-CCA2) and unforgeable against chosen-message attacks (EUF-CMA). And their scheme requires none of the recipient's public information in the offline phase and hence makes practical sense [10].

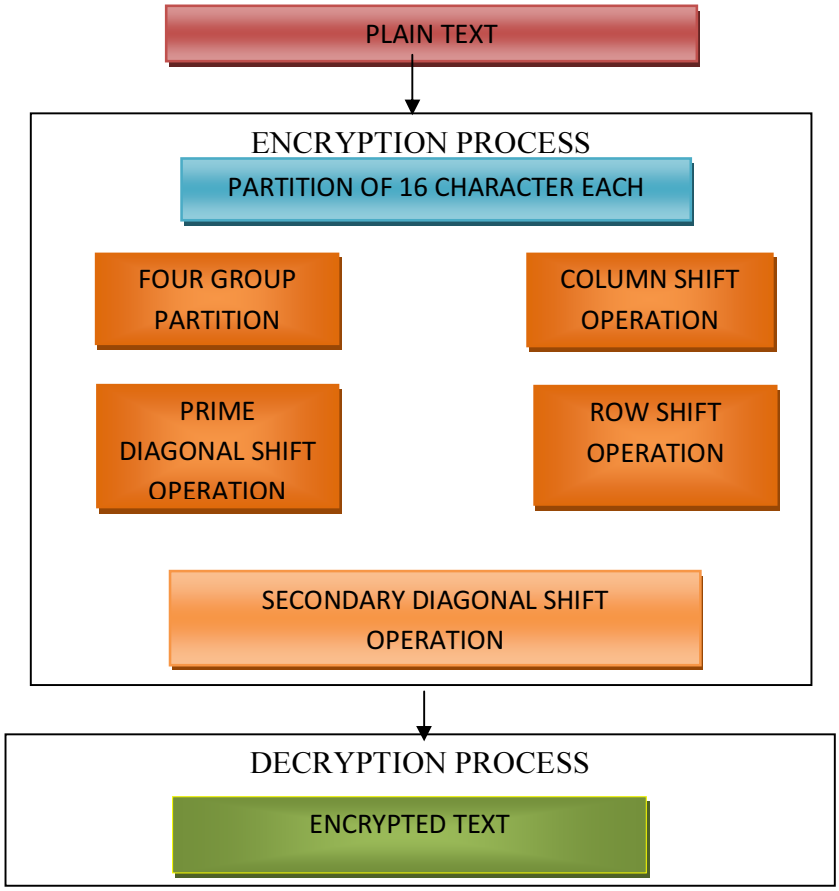
The Secure Hash Algorithm is one of the number of cryptographic hash functions.SHA-0:Aheteronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1.

SHA-1, A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be the part of Digital Signature Algorithm.SHA-2: A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA-256 uses 32-byte (256 bits) words where SHA-512 uses 64-byte (512 bits) words. There are also truncated versions of each standardized, known as SHA-224 and SHA-384. These were also designed by the NSA.

SHA-3:A hash function formerly called Keccak, chosen in 2012 by non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family. Because of the successful attacks on SHA-0, SHA-1,SHA-2, SHA-3 developed. It has output length as 512 – bit.

3. PROPOSED ARCHITECTURE

Based on challenges and opportunities, we proposed the following architecture for the process of keyless cryptography using the process of grid computing



Journal of Theoretical and Applied Information Technology
10th May 2014. Vol. 63 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.ALGORITHMIC STEPS

The following algorithm depicts the stepwise processes that are used in keyless cryptography using the process of grid computing.

- Step 1) Map the sequence S into a block having four columns and N/4 rows.
- Step 2) Perform Column shift in a certain specified order to the resulting symbol block
- Step 3) Perform Column shift in a certain specified order to the resulting symbol block
- Step 4)) Perform Prime Diagonal shift in a certain specified order to the block
- Step 5) Perform Secondary Diagonal shift in a certain specified order to the block obtained
- Step 6) Represent the outcome in a linear order to get the encrypted text.
- Step 7) Perform Secondary Diagonal shift in a order carried out in step5 to the Block obtained in step5
- Step 8) Perform Primary Diagonal shift in a order carried out in step4 to the Block obtained in step7
- Step 9) Perform Row shift in a order carried out in step 3 to the Block obtained in step8
- Step 10) Perform Column shift in a order carried out in step 2 to the Block obtained in step9
- Step11) Formulate the outcome in linear array to get the decrypted text

An illustration of how the proposed methodology is working out is given below.

Let the Given Plain Text be

ABCDEFGHIJKLMNOP

(One Partition of 16 characters)

1. Split them into four partition four character each

   ABCD EFGH IJKL MNOP

2. Arrange them in a matrix format to perform various shifting operation

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Perform Shift Operation 1 (Column Shift). Each column has to be shifted from top to bottom into a certain number of times. If column is shifted in the order [2 3 0 1] we get the output as follows

I	F	C	P
M	J	G	D
A	N	K	H
E	B	O	L

Perform Shift Operation 2 (Row Shift). Each Row has to be shifted from left to right into a certain number of times. If rows are shifted in the order [1,3,1,2] then the output will be as follows.

P	I	F	C
J	G	D	M
H	A	N	K
O	L	E	B

Perform Primary Diagonal Shift Operation 3. Each element of the primary diagonal should be shifted to a certain number of times from top to bottom. If such shifting is performed for 2 times then the following output will be the resulting outcome.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

N	I	F	C
J	B	D	M
H	A	P	K
O	L	E	G

Perform Secondary Diagonal Shift Operation 4. Each element of the secondary diagonal should be shifted to a certain number of times from top to bottom. If such shifting is performed for 3 times then the following output will be the resulting outcome.

N	I	F	D
J	B	A	M
H	O	P	K
C	L	E	G

The Encrypted text will be as follows

NIFDJBAMHOPKCLEG.

This is the output against the plain text message

ABCDEFGHIJKLMOP.

Once the cyclic transposition algorithm is applied on plain text, it leads to some of the cryptanalysis experts to make out some of the encryption patterns by working out combinational means yet. To make the encryption more complex and unpredictable, it is proposed to work out one more layer of encryption through the method of substitution. Special characters have been chosen for substitution. The character mapping table (Table 1)is given below. While decrypting the encrypted text, the exact reverse process is followed.

Table 1: Character Mapping Table

1	A	Chr(176)	16	P	Chr(225)	31	4	Chr(165)	46	j	Chr(15)
2	B	Chr(177)	17	Q	Chr(226)	32	5	Chr(164)	47	k	Chr(16)
3	C	Chr(182)	18	R	Chr(227)	33	6	Chr(162)	48	l	Chr(17)
4	D	Chr(184)	19	S	Chr(228)	34	7	Chr(155)	49	m	Chr(18)
5	E	Chr(187)	20	T	Chr(229)	35	8	Chr(149)	50	n	Chr(19)
6	F	Chr(191)	21	U	Chr(230)	36	9	Chr(139)	51	o	Chr(20)
7	G	Chr(216)	22	V	Chr(231)	37	a	Chr(2)	52	p	Chr(21)
8	H	Chr(217)	23	W	Chr(232)	38	b	Chr(3)	53	q	Chr(22)
9	I	Chr(218)	24	X	Chr(233)	39	c	Chr(4)	54	r	Chr(23)
10	J	Chr(219)	25	Y	Chr(234)	40	d	Chr(5)	55	s	Chr(24)
11	K	Chr(220)	26	Z	Chr(235)	41	e	Chr(7)	56	t	Chr(25)
12	L	Chr(221)	27	0	Chr(172)	42	f	Chr(8)	57	u	Chr(26)
13	M	Chr(222)	28	1	Chr(171)	43	g	Chr(236)	58	v	Chr(27)
14	N	Chr(223)	29	2	Chr(167)	44	h	Chr(12)	59	w	Chr(127)
15	O	Chr(224)	30	3	Chr(166)	45	i	Chr(14)	60	x	Chr(128)
61	y	Chr(134)	62	z	Chr(135)	CODE SHEET FOR SUBSTITUTION					

5. EVALUATION & PERFORMANCE ANALYSIS

The proposed architecture has been implemented in a grid environment. Gridsim [6] was used to generate simulation in the grid computing environment .A paragraph of plain text written in a word document has been produced to the input of this software. On Execution the output is obtained which is beyond the guessing of any intruder or expert as the output is simply like garbage. By

performing big O function lower and upper cases can be bound.Traditional algorithms like RSA and ECC use both private keys and public keys and hence there is a mandatory requirement of key handling managements, distribution and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

regeneration. All these tasks need some amount of resource consumptions in terms of time and space and utilization of CPU whereas CSTA does not require a key for all kind of resource consumption. This will be a great advantage of using CSTA over other conventional and traditional algorithms for nonexistence of key as such.

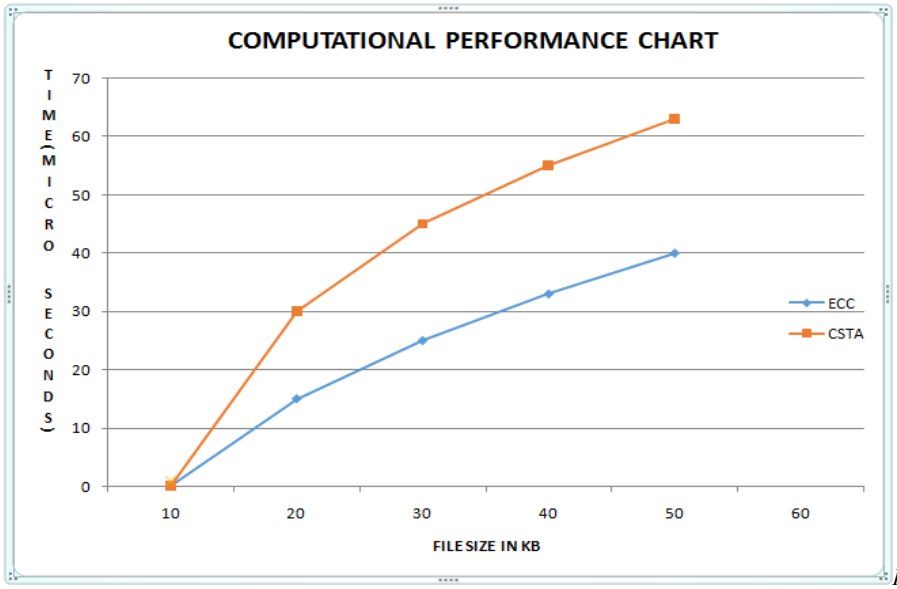


Figure 1: Computational Operations Between ECC And CSTA.

In terms of operations conventional algorithms such as RSA and ECC require a lot of computations in terms of arithmetic operations where CSTA does not use any such kind of computational operations instead of that it uses shift operations such as diagonal shifts column and row shifts etc. This in turn will help in achieving lesser utilization of resources. The ultimate performance has been computed to be a saving of 50 to 60 percent of computational overhead. The graph (Figure 1) given below provides a comparative computational operations between ECC and CSTA. The graph shows clearly that when the size of files grow (X axis), the computational time also grows yet one can observe that CSTA consumes lesser time than that of ECC.

6.RESULTS

Table 2 shows the performance in terms of HTTPS requests time over the increase of file size.

Table 2: HTTPS Requests Over File Size.

ALGORITHM	HTTPS REQUEST TIME(ms)	FILE SIZE IN KB
ECC-160	20	10
CSTA	14	
ECC-160	27	30
CSTA	16	

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6. CONCLUSION

In our paper, we proposed an effective Cyclic Shift Transposition Algorithm inorder to demonstrate the authenticity of incorporating it in the grid environment. It has also been covered under two heads. Simple text is being encrypted using CSTA and substituted as per the table mapping and conveyed in the grid to ensure grid authentication. The proposed algorithm is very effective in encrypting and decrypting a text file so that an intruder cannot make anything out of it once it is encrypted which in turn ensures data security.

REFERENCES:

[1] Amr Farouk, A.Ahmed, Abdelhafez, "Authentication Mechanisms in Grid Computing Environment: Comparative Study" international conference on ICET enieering and technology, pp.1-6, 2012.

[2] AnithaKumari.K ,"Trigon based Authentication, Authorization and distribution of encrypted keys with Globus midddleware" ,"International Journal of Computer Science and Information Security" vol 6, Dec 2009, pp (064-072).

[3] Baker.M, Buyya.R. andLaforenza.D , "Grids and Grid Technologies for Wide-area distributed Computing," Software-Practice & Experience, Vol. 32, No.15,2002, pp: 1437-1466.

[4] Bendahmane, A , AbdelmalekEssaa di "Grid computing security mechanisms: State-of-the-art "IEEE International Conference on Multimedia Computing and Systems, 2009, pp 535-540

[5] Boneh.D, Franklin.M,"Identity-based encryption from the Weil pairing". In: J.Kilian. (ed) Advances in Cryptology—Proceedings of CRYPTO 2001, LNCS, vol. 2139, Springer (2001),pp. 213–229

[6] Buyya.R and Murshed.M, "Gridsim: a toolkit for the modeling and simulation of distributed resource management and scheduling for grid computing," Concurrency and Computation: Practice and Experience,2002, vol. 14, pp. 1175–1220.

[7] Burruss.J.R,Fredian.T.W, Thompson.M.R, "ROAM: An Authorization Manager for Grids", Journal of Grid Computing", Volume 4, Issue 4, December 2006, pp 413-423.

[8] Chang et al ,"An Efficient Password Authentication Schemes Without Using the Server Public Key for Grid Computing",GCC 2005,pp 149-154.

[9] Faerman.M, Moore.R.W, Minster.B, Maechling.P, Cui.Y ,Hu,J.Zhu.Y, "Managing large scale data for earthquake simulations. ",Journal of Grid Computing, 2007.

[10] Fei Yan, Xiaofeng Chen, Yinghui Zhang "Efficient online/offline signcryption without key exposure",International Journal of of Grid and Utility Computing, 2013 ,Voume 4, No.1, pp.85 – 93

[11] Foster.I, Kesselman.C, (eds): The Grid 2: Blueprint for a New Computing Infrastructure. Elsevier, San Francisco (2004)

[12] Foster.I, Kesselman.C, Tsudik.G, Tuecke.S," A security architecture for computational Grids". In: Proceedings of the 5th ACM Computer and Communications Security Conference (CCS '98), pp. 83–92. ACM Press (1998)

[13] Guilin, Guangxi, "Research on User Authentication for Grid Computing Security "Second International Conference on Semantics, Knowledge, and Grid (SKG'06)