Asian Journal of Information Technology 12 (10): 318-324, 2013
ISSN: 1682-3915

Efficient Technique for Authentication and Integrity of Data in Grid Using CSTA

[1]R. Kalaiselvi and [2]V. Kavitha
[1]Department of Computer Science and Engineering,
Noorul Islam University, Tamil Nadu, India
[2]University College of Engineering, Nagercoil, Anna University,
Chennai, Tirunelveli Region, India

Abstract: Grid computing is a group of computer organizations from various fields which have joined together to achieve a common interest. A grid security issue is one of the main problem to grid computing. Security in terms of an authentication is a major issue in the Heterogeneous Grid System. Authentication is the process of confirming the identity of a person or a software program. In this proposed methodology, secure group communication is ensured to authenticated users by an effective key distribution using Cyclic Shift Transposition Algorithm (CSTA) which uses multiple key distributions during file or data transfer in a Grid System. In addition, Hash function incorporates authentication of users and resources in a grid environment. CSTA Algorithm when compared with other authentication algorithms like RSA, DES and AES, better results have been proven in terms of security and authentication.

Key words: Grid security, authentication framework, encryption, decryption, CSTA Model

INTRODUCTION

The main purpose of grid computing is sharing of resources. Grids are the super Internet for high-performance computing. Security is an important issue which needs a close understanding as grid computing. In the proposed methodology, secure group communication is ensured to authenticated users by effective key distribution using Cyclic Shift Transposition Algorithm (CSTA) in multiple key distributions. This CSTA scheme (Selvi and Kavitha, 2012) is an efficient method which is implemented over text file or data. This model consists of a equal number of rows and columns. All data is coded during initialization. The output from the engine is in the form of variable size words and the individual bit output corresponding to the inserted symbols cannot be determined, thus it is highly confidential. In addition, Hash function in the form of digital signature or certificate of authority is used to authenticate users and resources in the grid environment. CSTA algorithm with other authentication algorithms like RSA, DES and AES is also analyzed in this study.

LITERATURE REVIEW

An efficient algorithm (Hussain and Murthy, 2011) is proposed for solving the security issue. Grid computing has a problem like security of data, files system, backups, network traffic and host security. The concept is the digital signature with RSA algorithm, encrypts the data while transferring it over the network. A digital signature is a mathematical model to authenticate the digital message or document. A valid digital signature indicates that the message was created by a known sender and it was not altered during transmission.

The digital signature with the RSA algorithm scheme is to ensure the security of data in the grid. RSA algorithm is probably the most recognizable asymmetric algorithm. Till now, it is the only asymmetric (i.e., needs two different keys) algorithm used for private/public key generation and encryption. This includes both the digital signature scheme and the public key cryptography to enhance the security of grid computing.

The X.509 certificate (Kumari *et al*., 2011) for solving the authentication issue is proposed in another method of research. Most of the data intensive jobs and the computations that require access to the high-end recourses always involve grid computing because it helps the virtual organizations to share heterogeneous resources that are distributed at various geographic locations. Secure communication between entities is mandatory for any dynamic Virtual Organization (VO) which is formed using grids. Such computational grid whose entities share heterogeneous resources always incorporates certain features on authentication, authorization, non-repudiation, integrity, confidentiality

Corresponding Author: R. Kalaiselvi, Department of Computer Science and Engineering, Noorul Islam University, Tamil Nadu, India

and auditing. During transactions using grids some illegal users may try to break these features and try to access the resources to which their intervention is prohibited. A simple password authentication method is used to avoid such illegalities and this can be done by exchanging proxy credentials. Other than authentication; authorization and confidentiality should also be maintained. Specific users can access specific resources through proper channels with the help of authorization by mapping an entity to a grid map file. Presently grid technologies are using X.509 identity certificates to support user authentication and its usage in web service-based technologies on the grid is quite impossible.

Authentication plays a major role in grid security. Authentication is used to prevent external users from randomly accessing internal grid system. It refuses the external unauthorized users to protect the grid system from outside intruders. Authentication in the grid security module solves the security threats from the internal network when certificated grid users engage illegal operations within the grid. It also requires other grid system security protection measures. In this study (Guowen *et al*., 2010), the security grid authentication component adopts firewall features. Firewall is a better measure to protect user resources to ensure information security.

A password-based user authentication scheme (Lu *et al*., 2008) is used in another research article. This scheme is based on an Elliptic Curve Crypto System. This simple user authentication scheme has three different phases such as registration phase, authentication phase and password change phase. The drawback of this scheme is simpler, since it doesn't require either the symmetric encryption algorithm or the verification table. When the secret key of a server is known there won't be any security then there is no guarantee that the grid can be secured from attacks such as replay attack, on-line password guessing attack, off-line password guessing attack, etc.

An Open Grid Services Architecture (OGSA) is proposed (Mehta, 2004) to enable systems and their applications to run within the Distributed Systems. This grid service has many more elements which should be considered for Large-Scale Interoperable Systems. To describe this study, the authentication service is to be established between virtual organizations. In this research credential life span and renewal for authorized service credentials are not considered. The pre-distributed secret scheme or third-party scheme can be used to enable virtual organizations to authenticate each other and establish cryptographic keys for future secure communication. The study of this research describes the main requirements for authentication which are as follows: credential processing, authorization, credential conversion and identity mapping.

FRAMEWORK FOR AUTHENTICATION AND INTEGRITY USING CSTA

The process of authorization is distinct from that of authentication. Authentication is used to verify the identity of the sender. There are some types of techniques used in the authentication process. Hash function is one of the techniques which is mostly used to enhance the authentication process of a grid system. Here, authentication using the hash function has two processes:

- Authentication and integrity using Hash function during the encryption process
- Authentication and integrity using Hash function during the decryption process

Hash function during the encryption process: Authentication using Hash function on the encryption process is done at the sender side. The particular IP address of a system is selected from a grid pool. The grid pool contains a collection of resources used in a grid environment. This confirms the communicating system and sends the original message along with a key to CSTA encryption process. This gives the cipher message. Also, the Hash function process provides the Hash value of the original message. The Hash value and the cipher message is concatenated and then given to the receiver. The architecture framework for authentication using Hash function on encryption is shown in Fig. 1.

Hash function during the decryption process: authentication using Hash function on decryption is done at the receiver side. The received concatenated cipher message and Hash value is separated. Then, the cipher message along with a key is passed to CSTA decryption

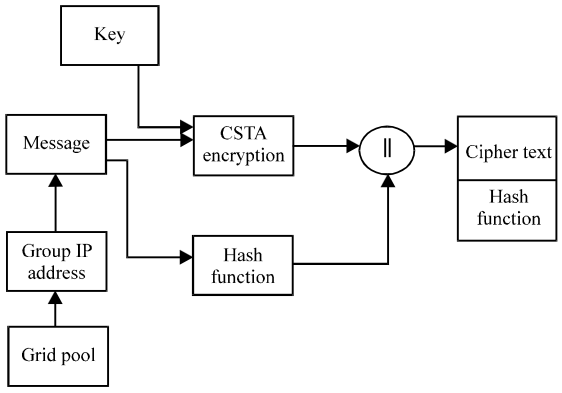


Fig. 1: Framework for authentication and integrity during the encryption process

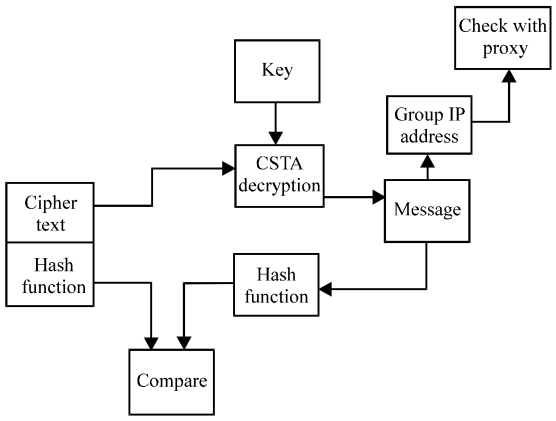


Fig. 2: Frame-work for authentication and integrity in the decryption process

approach. This decrypts the cipher message and produces the original message. The cipher message is passed to a Hash function process to obtain the Hash value of the decrypted message. Finally, both the hash values are compared. If any changes are obtained then the message is rejected. If there is no change of Hash values, then decrypted message is taken by that particular IP address of a resource. Also, it checks with the proxy of the resource. The architecture framework for authentication using Hash function on decryption is shown in Fig. 2.

Algorithm for CSTA encryption:

Input: The original text message
Step 1: Map the text sequence I into blocks of size,
N×N
Step 2: Perform column shift in a certain order specified
($C_k[C_{k1}\ C_{k2} \ldots C_{kn}]$)
Step 3: Perform row-shift in a certain order specified
($R_k[R_{k1}\ R_{k2} \ldots R_{km}]$)
Step 4: Perform primary diagonal shift in a certain order specified PD_k
Step 5: Perform secondary diagonal shift in a certain order specified SD_k
Step 6: Represent the outcome in a linear order to get the encrypted text
Output: Cipher text

Algorithm for CSTA decryption:

Input: The cipher text
Split the cipher text into blocks of size, N×N
Step 1: Perform secondary diagonal shift in a certain order specified
Step 2: Perform primary diagonal shift in a certain order specified
Step 3: Perform row shift in a certain order specified
Step 4: Perform column shift in a certain order specified
Step 5: Formulate the outcome in a linear order to get the decrypted text
Output: An original text message

CSTA MATHEMATICAL MODELING

Encryption process: Let the given input message as I which is given to a set of an even number of rows and columns as an N×N matrix:

$$I = [a_1 \ldots \ldots \ldots \ldots \ldots \ldots \ldots a_n]$$

Let I as I_e during the encryption process:

$$I_e = [a_1 \ldots \ldots \ldots \ldots \ldots \ldots \ldots a_n] \quad (1)$$

where, a to a_n is the elements of the message given as input. The elements from the input message is distributed evenly as rows and columns to the N×N matrix as:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ddots & a_{2n} \\ & & & \vdots \\ \cdots & \vdots & \cdots & \ddots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Where:

a_{11} = The first element of the input message
a_{mn} = The last element of the input message which is distributed in an N×N matrix according to the number of elements in the message

Key description: Keys are used to shift the elements from the N×N matrix. The key value is depended upon the number of elements in the N×N matrix is the form of 2^n. For example, consider the even N×N matrix is 4×4 matrix then the key size will be as 2^{10}. It is obtained by 4 keys for a column shift, 4 keys for a row shift, 1 key for the primary diagonal shift and 1 key for the secondary diagonal shift. If it is an 8×8 matrix then the key size will be as 2^{18}. It is obtained by 8 keys for the column shift, 8 keys for row shift, 1 key for the primary diagonal shift and 1 key for the secondary diagonal shift and so on. In this CSTA approach, researchers used four types of shifting processes. They are given as:

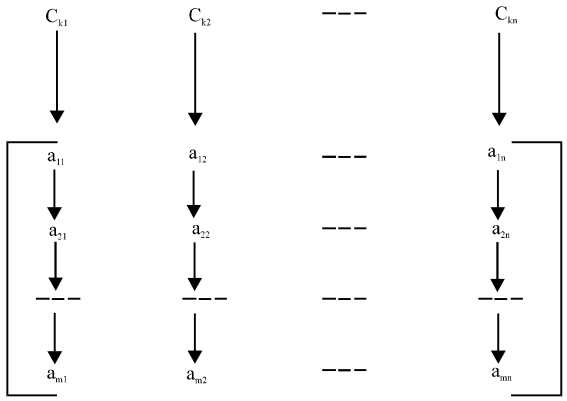
- Column shift
- Row shift
- Primary diagonal shift
- Secondary diagonal shift

Column shift: In the column shift the columns of N×N matrix are shifted according to the given key values in an N×N matrix. The keys for column shift are mentioned as C_k. Therefore, the keys for column shift will be as:

$$C_k = [C_{k1}\ C_{k2} \ldots C_{kn}]$$

Each key contains the integer value from 0-9. This integer key value which lies between 0-9 is given to the N×N matrix. According to the number of elements in the

N×N matrix, key values are given to each column. The keys given for a column shift of elements in an N×N matrix is shown as:

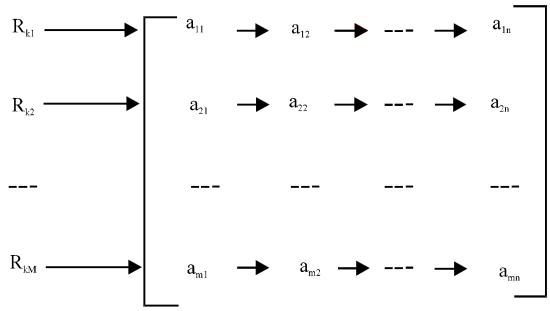


Here, the keys of C_k is distributed according to the elements in a N×N matrix. The elements from the N×N matrix is shifted its position by the given integer key value of C_k and produce a new N×N matrix. This new N×N matrix is used in the next process.

Rows shift: In the row shift, the rows of N×N matrix are shifted according to the given key values in N×N matrix. Keys for the row shift are mentioned as R_k. Therefore, keys for the row shift will be as:

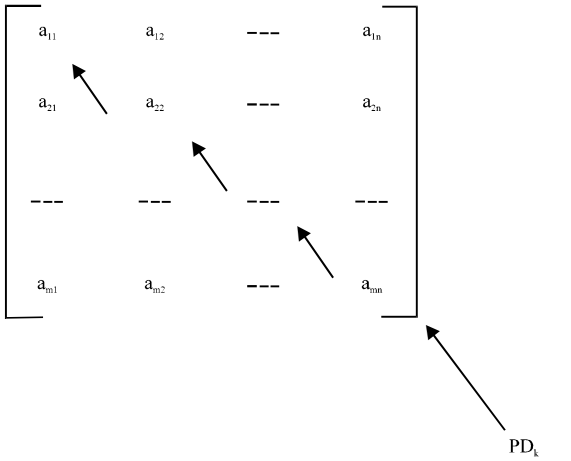
$$R_k = [R_{k1}\ R_{k2} \ldots R_{km}]$$

Each key contains the integer value from 0-9. This integer key value which lies between 0-9 is given to the N×N matrix. According to the number of elements in the N×N matrix key values are given to each row. The keys given for a row shift of elements in an N×N matrix is shown as:



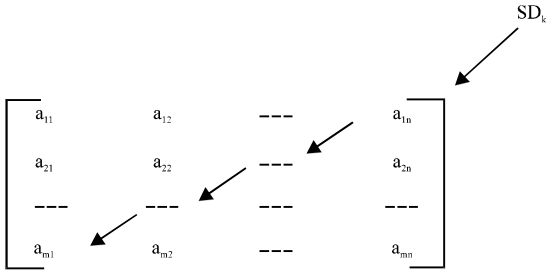
Here, the keys of R_k are distributed according to the elements in an N×N matrix. The elements from the N×N matrix is shifted its position by the given integer key value of R_k and produce a new N×N matrix. This new N×N matrix is used in the next process.

Primary diagonal shift: In the primary diagonal shift, diagonal from the right bottom to the left top (i.e., from a_{mn}-a_{11}) of the N×N matrix is shifted according to the given key value in an N×N matrix. The key for a primary diagonal shift is mentioned as PD_k which contains only one key value. The key contains the integer value from 0-9. This integer key value which lies between 0-9 is given to the N×N matrix. The primary diagonal shift key for elements of an N×N matrix is shown as:



The elements of the N×N matrix is shifted its position by the given integer key value of PD_k. This process produces a new N×N matrix and this new matrix is used for the next process.

Secondary diagonal shift: In secondary diagonal shift, the diagonal from the right top to left bottom (i.e., from a_{1n}-a_{m1}) of the N×N matrix is shifted according to the given key value in an N×N matrix. The key for secondary Diagonal shift is mentioned as SD_k which contains only one key value. The key contains the integer value from 0-9. This integer key value which lies between 0-9 is given to the N×N matrix. The key given for a secondary diagonal shift of elements in an N×N matrix is shown as:



The elements from the N×N matrix is shifted its position by the given integer key value of SD_k and produce a new N×N matrix. This new N×N matrix is used as the output matrix. The flow of the encryption process is shown as:

$$C_{kn} \rightarrow R_{km} \rightarrow PD_k \rightarrow SD_k$$

The elements of the N×N matrix which is derived from the secondary diagonal shift is the encrypted output message. This output message is used for decryption process.

Decryption process: The decryption process of CSTA approach is the exact reverse process of an Encryption process. The output N×N matrix from the secondary diagonal shift is taken an input. The flow of the decryption process is shown as:

$$SD_k \rightarrow PD_k \rightarrow R_{km} \rightarrow C_{kn}$$

The output elements from the column shift N×N matrix gives the original message elements which is given in the encryption process. This decrypted output is mentioned as I_d. Therefore:

$$I_d = [a_1 \ldots\ldots\ldots\ldots\ldots a_n] \quad (2)$$

Hash function: Hash function accepts a variable-size message M as input and produces a fixed-size output, referred as a Hash code H(M) (or) Hash value. Hash code does not use key, it is A variation on the message authentication code is the one-way hash function. As with the message authentication code, a function of the input message. The hash code is one of the function that has an error-detection capability. In general, the hash value 'h' is given in the following form:

$$h = H(M) \quad (3)$$

Where:
M = Variable-length message
H(M) = Fixed-length hash value

The authentication process of CSTA approaches a hash function to authenticate the message. CSTA approach to provide the message to the hash function is done by the given method.

Hash function for encryption: By using Eq. 1 and 3 the hash function for encryption is given as:

$$h_e = H(I_e)$$

Where:
h_e = Hash value for a function
I_e = Variable-length of a original input message
$H(I_e)$ = Fixed-length hash value for the original input message

Table 1: File size vs. CSTA encryption time

File size (kb)	Time taken (nsec)
8	120
16	140
24	160
36	180
40	200
48	220
56	240

Hash function for decryption: By using Eq. 2 and 3 the hash function for decryption is given as:

$$h_d = H(I_d)$$

Where:
h_d = Hash value for a function
I_d = Variable-length of a decrypted output message
$H(I_d)$ = Fixed-length hash value for the decrypted output message

EXPERIMENTAL SETUP

Implementation of CSTA based authentication and security in grid environment is done by two phases, one at sender side and the other at the receiver side. The sender sends a message and the receiver authenticates the sender and the message. In between CSTA based encryption is done at the sender side and decryption is done at the receiver side. The Hash value is generated by the sender and it is appended with original message. This value is compared with the receiver's hash value for the decrypted message. If both Hash values are same then the message and a sender will be authenticated in the grid environment. After the CSTA decryption process, original message is displayed at the receiver side. Then, the receiver selects the particular IP address and sends an acknowledgement to the sender that the message is received correctly without any error. Finally, the sender receives the acknowledgement from the receiver (Table 1).

PERFORMANCE EVALUATION

The performance evaluation has been made with other algorithms. The CSTA Algorithm gives better performance rather than other algorithms such as AES, DES and RSA. Initially, this accomplishes the partition operation by splitting the variable sized word (16 bit) into four partitions. Then, arrange them in a matrix format to perform various shifting operation. Following this, it maps the sequence into a block having four columns and four rows. Afterwards, perform the various shift operation such as diagonal shifting, row shifting and column shifting. Then, the sender side executes the encryption

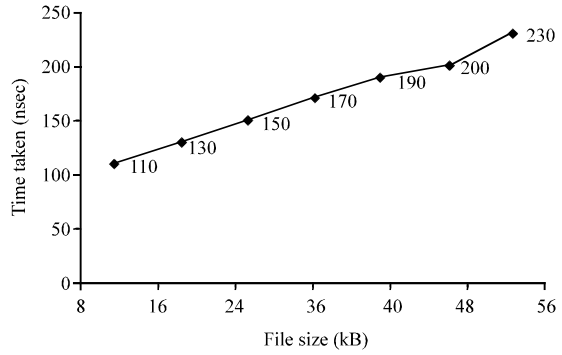


Fig. 3: Chart for file size vs. CSTA decryption time

Table 2: Comparison of RSA, AES, DES and CSTA

		No. of operations performed			
No. of characters	File types	RSA	AES	DES	CSTA
10	rtf	160	120	80	40
20	doc	320	240	160	80
30	txt	480	360	240	160
40	pdf	640	480	320	200

Table 3: Comparison for the various algorithm file size vs. time taken for encryption

	Time taken (nsec)			
File size (kB)	RSA	AES	DES	CSTA
10	600	450	300	150
20	1200	900	450	300
30	1800	1350	900	450
40	2400	1800	1200	600

operation by employing the cyclic shift transposition algorithm and hence forms the cipher text (16 bit). This cipher text is received by the receiver.

The decryption is performed by the receiver using the identical shifting operation and the partition operation. The decryption is the turn back process of encryption and then it obtains the original plain text. In the file operation the senders browse the files to be encrypted by selecting a particular folder. The files to be encrypted are uploaded and so the particular files are displayed in the select file for the encryption list box (Fig. 3).

Table 2 shows that RSA, AES, DES and CSTA for various file formats. The Results show that performance of CSTA is better than other existing algorithms. A set of characters in different file formats are compared with various types of algorithms such as RSA, AES, DES and CSTA. It is observed that CSTA has a less number of operational over head than other algorithms.

Table 3 show that the comparisons of a set of file size and time taken which is compared with various types of algorithms such as RSA, AES, DES, CSTA and its results show that performance of CSTA is better than other existing algorithms.

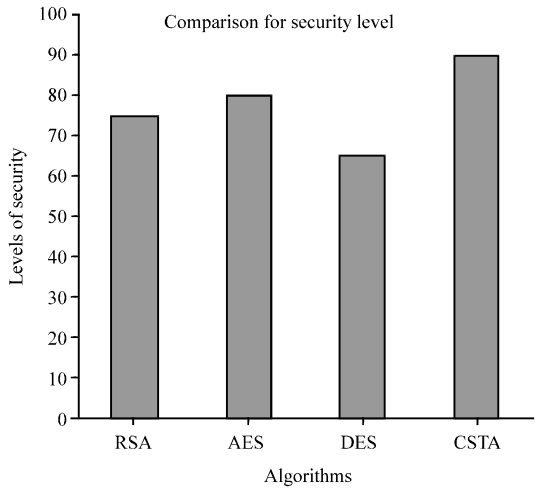


Fig. 4: Chart for security level

Figure 4 shows that the comparison of security level with various algorithms such as DES, AES, RSA, CSTA and the result showed CSTA is giving better performance rather than other algorithms.

CONCLUSION

The most effective cyclic shift transposition algorithm has been introduced to demonstrate how best authenticity can be incorporated in the grid environment. Simple of text is being encrypted using CSTA and conveyed in the grid to ensure grid authentication. Authentication of users and resources in a grid environment is done by providing a Hash function which gives for authentication to a grid environment. The most critical issue in grid is about handling of threats. Threats are emerging every day in new form and in new dimension. The most dangerous threat is intrusion in the network. An intruder will always try to have to access into grid resources with certain specific intention. It is therefore very important to protect the grid from intrusion. The algorithm proposed will even be encrypt and decrypt a text file so that an intruder cannot make anything out of it. The effective cyclic shift transposition algorithm can be enhanced for the usage of real-time video, audio and images during secure file transfer in Grid Environment System.

REFERENCES

Guowen, X., X. Shengjun and L. FangFang, 2010. Research of grid security authentication model subtitle as needed. Proceedings of the International Conference on Computer Application and System Modeling, Volume 1, October 22-24, 2010, Taiyuan, China, pp: 78-80.

Hussain, S.A. and K.E.S. Murthy, 2011. Information security by using signature with RSA encryption in grid computing. Int. J. Comput. Inform. Syst., Vol. 3.

Kumari, K.A., G.S. Sadasivam, R.S. Prabha and G. Saranya, 2011. Grid based security framework for online trading. Proceedings of the International Conference on Process Automation, Control and Computing, July 20-22, 2011, Coimbatore, India, pp: 1-4.

Lu, R., Z. Cao, Z. Chai and X. Liang, 2008. A simple user authentication scheme for grid computing. Int. J. Network Security, 7: 202-206.

Mehta, M., 2004. Authentication services in open grid services. Research Project Report, May 7, 2004.

Selvi, R.K. and V. Kavitha, 2012. Crypto system based authentication using CSTA in grid. Int. J. Comput. Appl., 48: 45-51.