Crypto System based Authentication using CSTA in Grid

R. Kalai Selvi
Associate Professor
Dept of CSE, Noorul Islam University
Kumaracoil .

V. Kavitha
PhD, Associate Professor
University College of Engineering, Nagercoil
AUT-Tirunelveli

ABSTRACT

Grid computing, as a distributed computing model, stands for the new kind of systems that pools heterogeneous computational resources, such as computers, storage space, sensors, application software, and experiment data. When a user wants to request some computing and data resources, the grid can seamlessly, transparently and dynamically supply them. The security issue has become an important concern of grid computing. To prevent the grid resources from being illegally visited, the strong mutual authentication is needed for user and server. In recent periods, many password-based user authentication schemes are proposed for solving the authentication issue. However, most of them are not ideal for grid computing, since they do not provide the strong mutual authentication. It is proposed to introduce an efficient user Cyclic Shift Transposition Algorithm (CSTA) scheme and a model for secure routing mechanism of sharing messages between source and destination in grid computing by adding information about sender and preserves the message content, which prevents not only known attacks but also maintains the integrity of data. This efficient method is implemented over text data. This model dynamically reorders the frequency of the input symbols according to the coupled cyclic shift system.All text 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 highly confidential.

General Terms

Grid Security, Authentication **,**Encryption ,Decryption.

Keywords

CSTA, Crypto system based Authentication.

1. INTRODUCTION

The cyclic shift transposition algorithm of a cryptographic application in Grid environment is to ensure authentication with respect to plain text only. It is also possible that an intruder may even take attempt to gain access control even in the WAN/LAN, Internet and Intranet Communication. In order to improve authentication, effective cryptographic methods can be introduced to ensure that an intruder does not get a chance to gain access to any form of network resources and if even in the event of gaining access, he should not be allowed to make it out the content of text encrypted. It is proposed to introduce an efficient user authentication cyclic shift transposition scheme and a model for secure routing mechanism of sharing messages between source and destination in grid computing. This efficient method is implemented in text file. In text operation variable sized word is used as plain text and in file operation 'n' number of word files can be used. The plain text message which is sent by the sender which has to be encrypted is subjected to partition operation by splitting the sentence in the file into variable sized word (16 bit), the empty space is also counted. Following this, it is subjected to shifting operation and therefore it forms the cipher text. This cipher text is received by the receiver. The cipher text received by the receiver requires being decrypted to incur the original plain text. This decryption is performed using the identical cyclic shift transposition algorithm. The decryption is the turn back process of encryption and hence it obtains the plain text. The cryptology techniques may be incorporated to overcome problems in security issues. As an enhancement to the proposed work, one can think of working strategies of application of same or slightly modified algorithm for the application of encryption and decryption in other form files such as images, audio and video etc.

2. RELATED WORK

According to Rongxing Lu, et all have proposed password-based user authentication schemes are proposed for solving the authentication issue [4]. A new password based user authentication scheme based on the elliptic curve cryptosystem was proposed. The Password based simple user authentication scheme for grid computing consist of three phases: the registration phase, the authentication phase and the password change phase. The drawback of this scheme is simpler, since it doesn't require either the symmetric encryption algorithm or the verification table. 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. However, most of them are not ideal for grid computing, since they are based on smart card and do not provide the strong mutual authentication.

According to Qinghua Li and Guohong Cao [2] multicast authentication has been envisioned to be useful in many Smart Grid applications such as demand-response, wide area protection, in-substation protection, and various operation and control. Since the multicast messages are related to critical control, authentication is necessary to prevent message forgery attacks. Based on these requirements, we find that heavy signing light verification (HSLV) and Light Signing Heavy Verification (LSHV) is a promising solution, due to its short authentication delay and low computation cost. HSLV with LSHV are combined to form a new scheme Tunable Signing and Verification (TSV) which achieves a flexible tradeoff between the two. The most straight forward solution to multicast authentication is to use public key cryptography (PKC) based on digital signatures like RSA.

In the paper of Chong-Yen Lee, et all [3] the Grid computing architecture was defined to be a complete physical layer. Data transfer in network is insecure. In this study, encryption and decryption algorithms of a site authentication and its message are developed and applied in each grid node to ensure secure information transformation. If the site information has been built in the supervisor node then it can receive data sent from other grid nodes in secure way. Message processing can be kept in secure for all systems when these algorithms are installed in all nodes. This scheme has proposed a dynamic supervising model .

Jingshu Chen et all [5] has insisted that the authentication technologies in the grid computing environments can successfully assure the valid authentication, but they cannot meet the stress of new security challenges in grid environment, such as flexibility, lightweight, and extensibility. In sequence to satisfy the refuge needs of the computational grid, this paper has proposed a reflective authentication framework. This scheme provides better customizing ability and adaptive ability of platform.

In the paper V.Kavitha et all [1], existing system uses password based user authentication and arithmetic coding scheme concepts. The password based user authentication is setup by user choosing the password and the Hash of password is stored in password file. There is no Attacks such as Online dictionary attack in which the user guess passwords and try to log in, Offline dictionary attack is done by Stealing password file, try to find password with hash of password in file, Typical password dictionary. It may be entries of common passwords such as people's names, common pet names, and ordinary words. Dictionary attack in at most 100,000 seconds = 28 hours, or 14 hours on average. This scheme has some drawbacks, because it is not guarantee that the grid can be secured from attacks such as Replay attack, On-Line Password Guessing Attack, Off-Line Password Guessing attack, etc.

3. ARCHITECTURE FOR AUTHENTICATION

Authentication is one of the verification processes of identification of a person in grid security. It also provides interfaces to plug-in different authentication mechanisms and means to convey the mechanism used. The security of a Grid computing system in improved by means of enhancing the authentication techniques. The authentication can be achieved by three ways. The three ways are

1. Password based Algorithm
2. Cryptography based Algorithm
3. Hash function

Password based Algorithm: The Password based Algorithm can be improved by two methods such as Kerberos Authentication and SSL Authentication. Kerberos is an authentication service designed for use in a distributed environment. It makes use of a trusted third party authentication service that enables clients and servers to establish authenticated communication. The internet standard version is called transport layer service. SSL provides confidentiality using symmetric encryption and message integrity using message authentication code.

Cryptography based Algorithm: The cryptography based algorithm is of two types. One is public key algorithm and the other is secret key algorithm. Pair of keys has been selected so that if one is used for encryption the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

Hash function: Third way is the hash function, which can be done either by digital signature or certificate authority. Digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash function of the message and encrypting the message with creator's private key. The signature guarantees the source and integrity of the message. The user certificates are assumed to be created by some trusted certification authority and placed in the directory by the Certificate Authority (CA) or by the user. The directory server itself is not responsible for the creation of public keys or for the certification function. User certificates generated by a CA must be any user with access to the public key of the CA can verify the user public key that was certified. No party other than the certification authority can modify the certificate without this being detected. The architecture view of authentication is shown in figure 1.

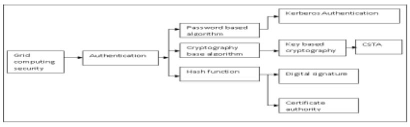


Fig 1: Grid Architecture for authentication

4. CRYPTOSYSTEM BASED AUTHENTICATION

In this proposed scheme an efficient user authentication is introduced. This algorithm performs four main operations such as partition, shifting, and encryption & decryption operation. The proposed CSTA method is based on cryptography based authentication algorithm. It can be done by Cyclic Shift Transposition Algorithm, which can be either public key algorithm method or secret key based algorithm based on the key selection of the users during the encryption and the decryption process.

4.1 Encryption Process

The sender affords the input text for encryption in the text operation or file operation. Initially, the algorithm accomplishes the partition operation by splitting the sentences into a variable sized word (16 bit) and then into four partition that is to say; in other words into four character. 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 N/4 rows. Afterwards, perform the shift operation 1(Column shift) in a certain specified order to the resulting symbol block needed. Subsequently, it performs the Shift Operation 2 (Row Shift). Each Row has to be shifted from left to right into a certain number of times. Later on, it perform shift operation3 (Primary Diagonal Shift Operation) Each element of the primary diagonal must be shifted to a definite number of times from top to bottom. Then, perform the shift operation 4(Secondary Diagonal Shift Operation) in which each element of the secondary diagonal must be shifted to a certain number of times from top to bottom. This encrypted form of text is the cipher text which should be sent to the receiver by the sender. The Encryption process is shown in figure 2.

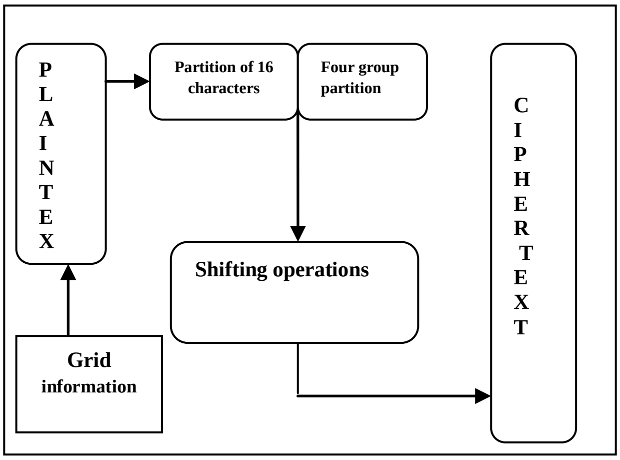


Fig .2: Encryption Process

4.2 Decryption Process

The cipher text received by the receiver requires being decrypted to incur the original plain text. This decryption is performed using the identical shifting operation and then supposed to perform the partition operation to perform the identical cyclic shift transposition algorithm. The decryption is the turn back process of encryption and hence it obtains the plain text. This process is shown in figure3.

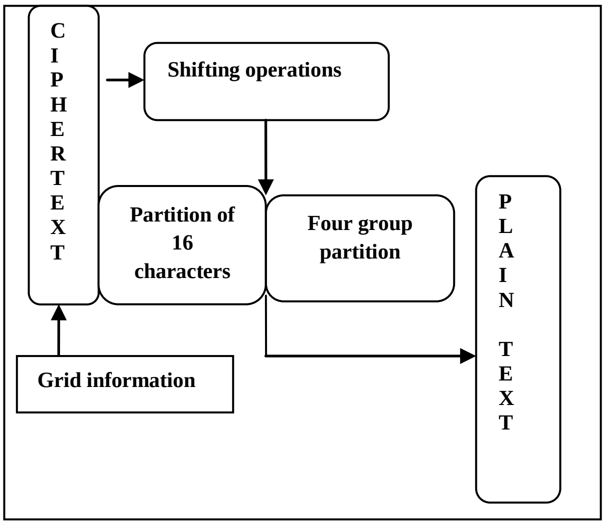


Fig 3: Decryption Process

4.3 Cyclic Shift Transposition Algorithm

The functionality of this algorithm in grid architecture is explained as follows: Initially, a grid computing system is to enhance the security of information from the sender which is then subjected to encryption process. The encryption process consists of partition operation and then it is subjected to shifting operation and thus it obtains the cipher text. The cipher text is converted to the original plain text by the receiver by performing the identical reverse process.

In partition operation the block of the plain text is subjected to splitting with variable sized word and then subjected to shifting operation. The shifting operation is as follows.

Algorithm1: CSTA Encryption

```
Input: Text Message.
Step1: Map the Text sequence S into blocks of size NxN.
Step2: Perform shift column in a certain order specified (CS [xxxx]).
Step3: Perform shift row in a certain order specified (RS [xxxx]).
Step4: Perform prime Diagonal shift in a certain order
         specified $D_1[x]$.
Step5: Perform secondary Diagonal shift in a certain order
         specified $D_2[x]$.
Step6: Represent the outcome in a linear order to get the
       encrypted text.
Output: Ciper text.
```

Algorithm2: CSTA Decryption

```
Input: Ciper text.
Split the cipher text into blocks of size NxN.
Step1: Perform Secondary Diagonal shift in an order
         carried out.
Step2: Perform prime Diagonal shift in an order carried out
         in a certain order specified.
Step3: Perform Row shift in a certain order specified.
Step4: Perform Column shift in an certain order specified.
Step5: Formulate the outcome in a linear order to get the
       decrypted text.
Output: Text Message.
```

Main advantages of the proposed system are

1. The model dynamically reorders the frequency of the input symbols according to the coupled cyclic shift system.
2. All text that has been coded since the initialization of the model.
3. The output from the engine is in the form of variable sized words and the individual bit output corresponding to inserted symbols cannot be determined.
4. Security has been enhanced using a new cryptographic approach.

5. IMPLEMENTATION METHODOLOGY

The proposed CSTA algorithm is implemented over text file based on word and group of words. The file format consists of two processes.

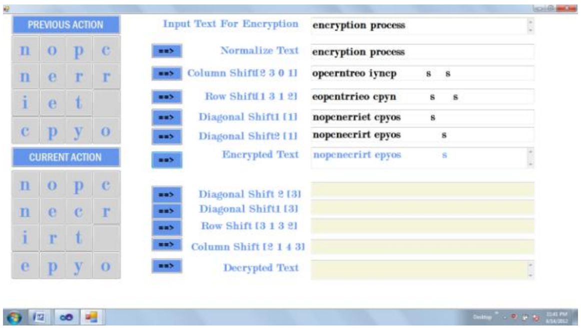
The sender affords the input text for encryption in the text operation. Initially, the algorithm accomplishes the partition operation by splitting the variable sized word (16 bit) into four partition that is to say; in other words into four character. Then, arrange them in a matrix format to perform various shifting operation. Following this, it maps the sequence into a block having four columns and N/4 rows. Afterwards, perform the shift operation 1(Column shift) in a certain specified order to the resulting symbol block needed. Subsequently, it performs the Shift Operation 2 (Row Shift). Each Row has to be shifted from left to right into a certain number of times. Later on, it perform shift operation3 (Primary Diagonal Shift Operation) Each element of the primary diagonal must be shifted to a definite number of times from top to bottom. Then, perform the shift operation 4(Secondary Diagonal Shift Operation) in which each element of the secondary diagonal must be shifted to a certain number of times from top to bottom. This encrypted form of text is the cipher text which should be sent to the receiver by the sender.

The receiver affords the cipher text for decryption in the text operation. This decryption is performed using the identical shifting operation and then supposed to perform the partition operation to perform the identical cyclic shift transposition algorithm. The decryption is the turn back process of encryption and hence it obtains the plain text.

In the file format, the sender side uploads the demanded files. The sender can upload ‘n’ number of files. Then the sender side executes the encryption operation by employing the cyclic shift transposition algorithm and hence forms the cipher text. This algorithm carries out the partition operation by splitting the sentence in the files into variable sized word (16 bit), the empty space is also counted. Following this, it is subjected to shifting operation and therefore it forms the cipher text. This cipher text is received by the receiver. The cipher text received by the receiver requires being decrypted to incur the original plain text. This decryption is performed using the identical shifting operation and then supposed to perform the partition operation to perform the identical cyclic shift transposition algorithm. The decryption is the turn back process of encryption and hence it obtains the plain text.

6. PERFORMANCE EVALUATION

The simulation tool used in our proposed method is gridsim. Simulation appears to be the only feasible way to analyze algorithms on large-scale distributed systems of heterogeneous resources. By using Gridsim, they are able to perform repeatable experiments and studies that are not possible in real dynamic Grid environment.



PREVIOUS ACTION

n	o	p	c
n	e	r	r
i	e	t	
c	p	y	o

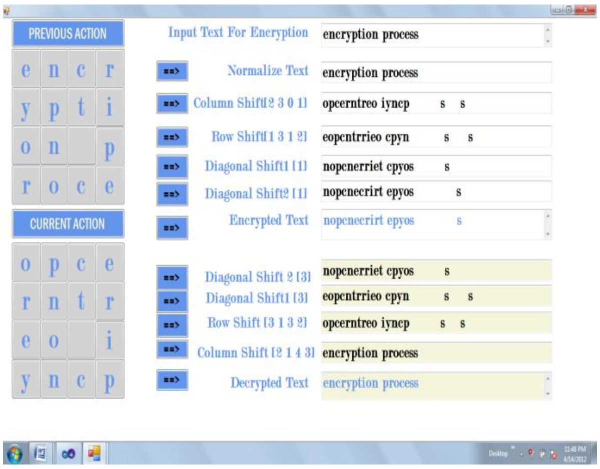
CURRENT ACTION

n	o	p	c
n	e	c	r
i	r	t	
e	p	y	o

Input Text For Encryption: encryption process
Normalize Text: encryption process
Column Shift[2 3 0 1]: opcerntreo iyncp   s   s
Row Shift[1 3 1 2]: eopcntrrieo cpyn   s   s
Diagonal Shift1 [1]: nopcnerriet cpyos   s
Diagonal Shift2 [1]: nopcnecrirt epyos   s
Encrypted Text: nopcnecrirt epyos   s
Diagonal Shift 2 [3]:
Diagonal Shift1 [3]:
Row Shift [3 1 3 2]:
Column Shift [2 1 4 3]:
Decrypted Text:

Fig.4: Perform the operations to form the encrypted

Initially, the algorithm accomplishes the partition operation by splitting the variable sized word (16 bit) into four partition. 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, column shifting and row shifting. Thus it forms the plain text



PREVIOUS ACTION

e	n	c	r
y	p	t	i
o	n		p
r	o	c	e

CURRENT ACTION

o	p	c	e
r	n	t	r
e	o		i
y	n	c	p

Input Text For Encryption: encryption process
Normalize Text: encryption process
Column Shift[2 3 0 1]: opcerntreo iyncp   s   s
Row Shift[1 3 1 2]: eopcntrrieo cpyn   s   s
Diagonal Shift1 [1]: nopcnerriet cpyos   s
Diagonal Shift2 [1]: nopcnecrirt epyos   s
Encrypted Text: nopcnecrirt epyos   s
Diagonal Shift 2 [3]: nopcnerriet cpyos   s
Diagonal Shift1 [3]: eopcntrrieo cpyn   s   s
Row Shift [3 1 3 2]: opcerntreo iyncp   s   s
Column Shift [2 1 4 3]: encryption process
Decrypted Text: encryption process

Fig.5: The encrypted ciper text is subjected to all the identical operations to obtain the original plain text.

The decryption is performed by the receiver using the identical shifting operation and then supposed to perform the partition operation to perform the identical cyclic shift transposition algorithm. The decryption is the turn back process of encryption and hence it obtains the plain text.

In the file operation the sender browse the files to be encrypted by selecting particular folder.

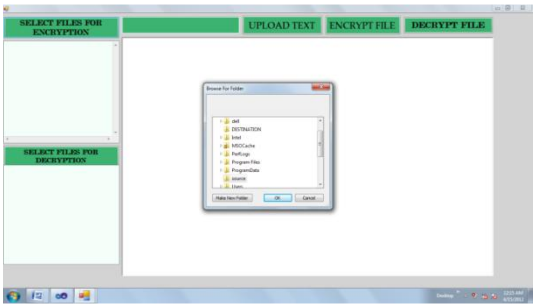
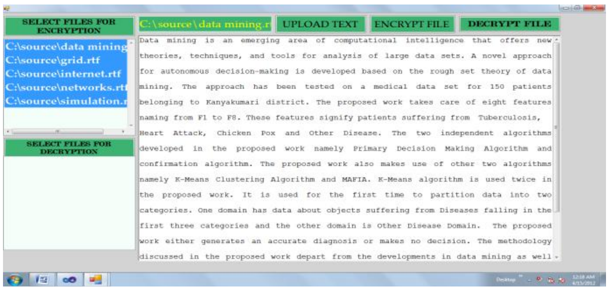


Fig.6: Browse the folder to obtain the required files to perform the Encryption Process.



C:\source\data mining.r

C:\source\data mining
C:\source\grid.rtf
C:\source\internet.rtf
C:\source\networks.rtf
C:\source\simulation.r

```
Data mining is an emerging area of computational intelligence that offers new
theories, techniques, and tools for analysis of large data sets. A novel approach
for autonomous decision-making is developed based on the rough set theory of data
mining. The approach has been tested on a medical data set for 150 patients
belonging to Kanyakumari district. The proposed work takes care of eight features
naming from F1 to F8. These features signify patients suffering from Tuberculosis,
Heart Attack, Chicken Pox and Other Disease. The two independent algorithms
developed in the proposed work namely Primary Decision Making Algorithm and
confirmation algorithm. The proposed work also makes use of other two algorithms
namely K-Means Clustering Algorithm and MAFIA. K-Means algorithm is used twice in
the proposed work. It is used for the first time to partition data into two
categories. One domain has data about objects suffering from Diseases falling in the
first three categories and the other domain is Other Disease Domain.  The proposed
work either generates an accurate diagnosis or makes no decision. The methodology
discussed in the proposed work depart from the developments in data mining as well
```

Fig.7: Uploads the files for encryption process

The files to be encrypted are uploaded and so the particular files are displayed in the select file for encryption list box**.**

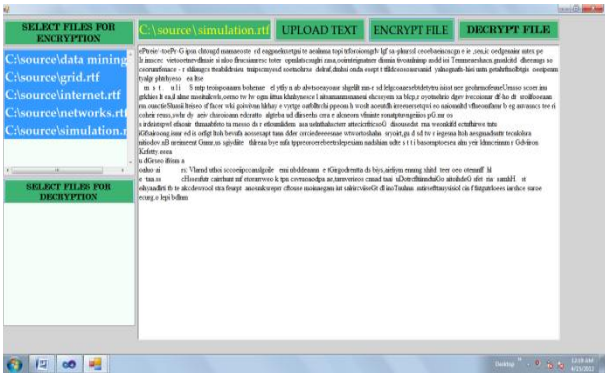


Fig.8:The plain text in the files are encrypted to form the cipher text.

Then the sender side executes the encryption operation by employing the cyclic shift transposition algorithm and hence forms the cipher text. This algorithm carries out the partition operation by splitting the sentence in the files into variable sized word (16 bit), the empty space is also counted. Following this, it is subjected to shifting operation and therefore it forms the cipher text. This cipher text is received by the receiver.

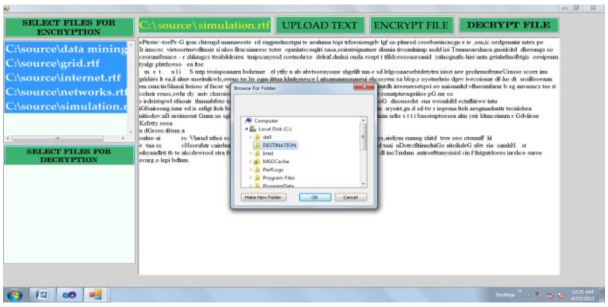
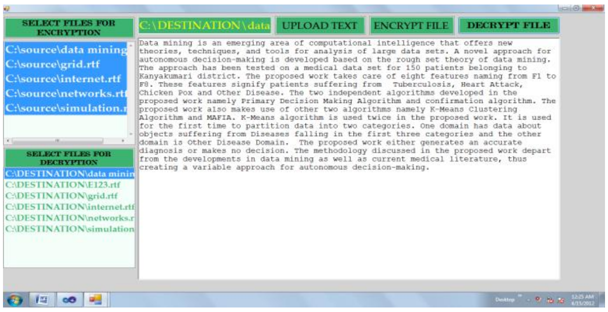


Fig.9:Browse a folder to save all the encrypted files.

The path is browsed to save all the encrypted file and so all the files are get saved after converting into cipher text.



```
Data mining is an emerging area of computational intelligence that offers new
theories, techniques, and tools for analysis of large data sets. A novel approach for
autonomous decision-making is developed based on the rough set theory of data mining.
The approach has been tested on a medical data set for 150 patients belonging to
Kanyakumari district. The proposed work takes care of eight features naming from F1 to
F8. These features signify patients suffering from  Tuberculosis, Heart Attack,
Chicken Pox and Other Disease. The two independent algorithms developed in the
proposed work namely Primary Decision Making Algorithm and confirmation algorithm. The
proposed work also makes use of other two algorithms namely K-Means Clustering
Algorithm and MAFIA. K-Means algorithm is used twice in the proposed work. It is used
for the first time to partition data into two categories. One domain has data about
objects suffering from Diseases falling in the first three categories and the other
domain is Other Disease Domain.  The proposed work either generates an accurate
diagnosis or makes no decision. The methodology discussed in the proposed work depart
from the developments in data mining as well as current medical literature, thus
creating a variable approach for autonomous decision-making.
```

Fig.10:The encrypted files are subjected to perform the identical operation by the receiver to obtain the original files.

The cipher text received by the receiver requires being decrypted to incur the original plain text. This decryption is performed using the identical shifting operation and then supposed to perform the partition operation to perform the identical cyclic shift transposition algorithm. The decryption is the turn back process of encryption and hence it obtains the plain text.

Table I: File Size Vs Encryption Time

File Size (KB)	Time Taken
8	120
16	140
24	160
36	180
40	200
48	220
56	240

Encryption time in nanosec Vs File size in kilobytes graph is shown in Figure 11.In the encryption process randomly assign different file size and then note the time utilized for the encryption of the file based on the CPU usage.

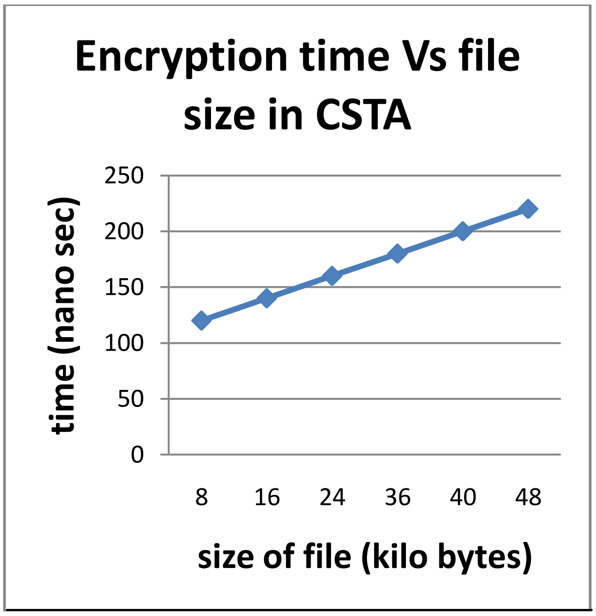


Fig. 11: Encryption time Vs File size

Table II: File size Vs decryption time

File Size	Time taken (ns)
8	110
16	130
24	150
36	170
40	190
48	210
56	230

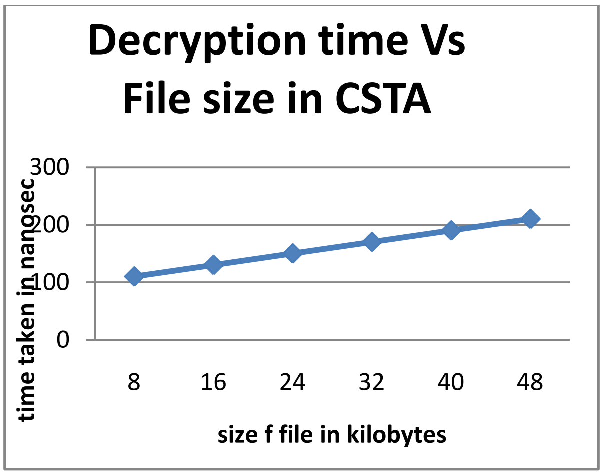


Fig.12 : File size vs Decryption time .

Decryption time in nano sec Vs File size in kilobytes graph is shown in figure 12. In the decryption process randomly assign different file size and then note the time utilized for the decryption of the file based on the CPU usage.

Table III: Comparison of RSA, AES, HMAC, CSTA

Table III shows the comparison of different algorithms such as RSA,AES,HMAC,CSTA for various file formats. Results show that performance of CSTA is better than other existing algorithms.

No.Of Char-cter	File types	No. of operations performed			
		RSA	AES	HMAC	CSTA
1	rtf	16	12	8	4
2	doc	32	24	16	8
3	txt	48	36	24	16
4	pdf	64	48	32	20

A set of characters in different file formats is compared with various types of algorithms such as RSA, AES, HMAC, CSTA and the results are shown in Figure 13. It is observed that CSTA has less complexity & less number of operational overhead than other algorithms.

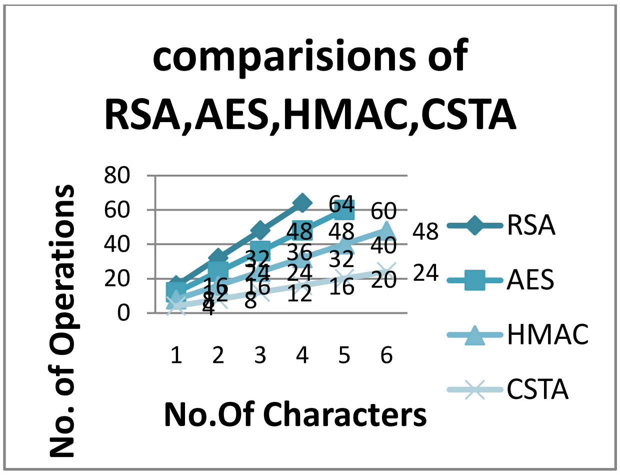


Fig13: Comparison of various algorithms.

5. 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. 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. Data is the most crucial component and any such leakage of sensitive data will result in a grave damage to individuals. Data pertaining to National security, sensitive information about the capability of defence forces are not supposed to fall on the hands of foreign intruders. It is therefore very important to protect our 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. A topic of future work is the development of algorithms that allow more authentication techniques to improve working strategies of application of same or slightly modified algorithm for the application of encryption and decryption in other form files such as images like fingerprints etc.

6. REFERENCES

[1] Dr. V.Kavitha et all. “ESAC Based Channel Aware Routing Using Route Handoff”International Journal on Computer Science and Engineering (IJCSE)in Vol.3. No.3 March 2011,Page No.1260-1269.

[2] Qinghua Li, *Student Member*, *IEEE*, Guohong Cao, *Fellow*, *IEEE*,Multicast Authentication in Smart Grid With One-Time Signature”

[3] Chong-Yen Lee et all. “Secure Site Authentication and Message Transmission Based on Grid Environment”, Fifth International Joint Conference on INC, IMS and IDC. 2009

[4] Rongxing Lu et all. “A Simple User Authentication Scheme for Grid Computing” International Journal of Network Security, Vol.7, No.2, PP.202–206, Sept. 2008.

[5] Jingshu Chen1 et all,” The Authentication Technologies in the Grid Computing Environment”, Computer Network Information Center, Chinese Academy of Sciences, Beijing 100080, China.

[6] Mostafa M. Fouda et all, “A Lightweight Message Authentication Scheme for Smart Grid Communications” IEEE Transactions on Smart Grid , Vol. 2, No. 4, Page. No. 675-685 DECEMBER 2011.

[7] Manish Metha,” Authentication Services in Open Grid Services” Research Project Report, May 2004.

[8] Xing guowen et all.,”Research of Grid Security Authentication Model Subtitle as needed” International Conference on Computer Application and System Modeling (lCCASM 2010) Vol.1,Page No. 78 -80.

[9] Jan Wiebelitz,”TCP-AuthN: TCP Inline Authentication to Enhance Network Security in Grid Environments”,Eighth International Symposium on Parallel and Distributed Computing 2009.

[10] Spillman, R.J.”Classical and Contemporary Cryptology. Upper Saddle River, NJ: Pearson Prentice-Hall.

[11] Balaji.R, Roopak .V, “Dynamic Password Authentication and Security System using Grid Analysis”, IEEE Commun. Surveys & Tutorials, vol.PP, no.99, pp.1-24, 2010.

[12] Jingshu Chen, Hong Wu, Qingyang Wang, Qingguan Wang, Xuebin Chi, “A Reflective Framework for

Authentication in Grid Computing Environments”, IEEE

Transactions on grid., vol 20, no 5, pp 324-335, May 2008.