Emphasize the Cloud Security Using Various Substitution Techniques

P Rajashekar, D. Aruna Kumari, PKVS Sarma, Y Prabhu Kumar

Abstract: Cloud computing is the technology used for storing the Information and packages on faraway servers and accessing them through the net rather than saving or installing them to your non-public or office pc. The time period cloud is used because information and programs are saved on a cloud or collection of web servers and computers owned by a third party. Most issues start from the fact that the person loses manipulate of his or her records, because it's miles stored on a laptop belonging to a person else (the cloud provider). Cloud Computing affords a platform with an superior and efficient way to store statistics inside the cloud. The functioning of Cloud Computing is significantly distressed with the aid of problems including that of statistics safety, integrity, theft, loss and presence of inflamed applications. These troubles are the important dangers to the consumer to transport their statistics to the cloud. we have analyzed various Substitution techniques to attain high level of security to cloud storage.

Keywords: Cloud, Plain text, Cipher text, Encryption, Decryption, Cryptography, Security, Key.

I. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. Where within the past, humans might run packages or applications from software downloaded on a physical laptop or server in their constructing, cloud computing allows humans to access the same styles of packages via the net. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. All you need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc.

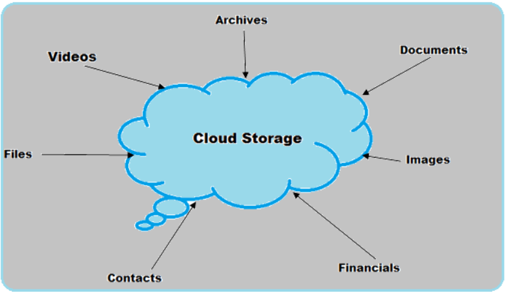


Fig. 1.Cloud Storage

Revised Version Manuscript Received on 16 September, 2019.

* Correspondence Author
P Rajashekar, Asst Professor, Department of CSE, Vidya Jyothi Institute of Technology,HYD Email: rajashekar@vjit.ac.in
Dr.D.Aruna Kumari , Professor, Department of CSE, Vidya Jyothi Institute of Technology,HYD, arunakumari@vjit.ac.in
PKV Sarma, Asst Professor, Department of CSE, Vidya Jyothi Institute of Technology,HYD Email: sarma@vjit.ac.in
Y Prabhu Kumar Department of CSE, VJIT, Hyderabad ,Telangana,India . prabhukumar@vjit.ac.in

1.1 Advantages of Cloud:

Usability: All cloud storage services reviewed in this topic have work area envelopes for Mac's and PC's. This enables clients to move documents between the distributed storage and their local storage.

Bandwidth: You can avoid emailing files to individuals and instead send a web link to recipients through your email.

Accessibility: Stored files can be accessed from anywhere via Internet connection.

Disaster Recovery: It is highly recommended that businesses have an emergency backup plan ready in the case of an emergency. Cloud storage may be used as a back-up plan by using groups by means of supplying a 2nd reproduction of essential documents. These files are stored at a remote location and can be accessed through an internet connection.

Cost Savings: Businesses and organizations can often reduce annual operating costs by using cloud storage; cloud storage costs about 3 cents per gigabyte to store data internally. Users can see additional cost savings because it does not require internal power to store information remotely.

II. RELATED WORK

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers[1,2].

There are four main basic objectives of cryptography:

1) *Confidentiality:* The information cannot be understood by anyone for whom it became accidental.

2) *Integrity*: The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

3 Non-repudiatio Integrity: The data can not be modified in carport or travel among sender and implied recipient without the change being detectedn

4) Verification: The sender and recipient can affirm each other's personality and the birthplace/goal of the data

.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

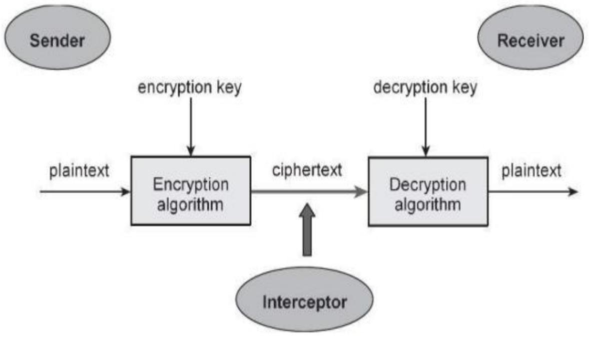


Fig. 2. Cryptography Block Diagram

There are two principal classes of cryptography depending at the form of security keys used to encrypt/decrypt the information. These two classes are: Symmetric and Asymmetric encryption techniques. This capability surmounts the symmetric encryption trouble of handling mystery keys. But however, this particular characteristic of public key encryption makes it mathematically greater at risk of attacks. Moreover, uneven encryption techniques are almost 1000 instances slower than symmetric techniques; because they require more computational processing energy. Cryptography is an artwork and science of converting unique message into non readable shape. From the encryption set of rules factor of view, there are most important strategies we used to implement within the secret key cryptography (symmetric cipher) gadget: Substitution cipher and Transposition cipher.

In this paper, we have analyzed and start the discussion on various substitution techniques on the basis of cryptanalysis and possibility of attack. This analysis gives some better results about comparison among these substitution techniques to provide more security and privacy of data in cloud storage [2].

III. SUBSTITUTION TECHNIQUES

Substitution process in the field of network security is an easy and more secure strategy for send ing e-mails. Parts of actual data will be replaced with fixed framework
There are various kinds of substitution figure.

- ***CAESAR* cipher,**
- **polygraphic**
- **monoalphabetic cipher**
- **polyalphabetic cipher**

1. CAESAR CIPHER

In this approach ,Ciper text will be generated with a fixed number . for example, If the number is 2 , then A will be adjunct by C and X will be adjunct by Z.

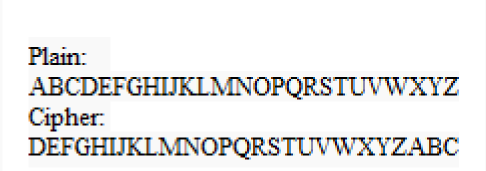
The encryption can likewise be spoken to utilizing secluded number-crunching by changing the data into numeric, with the help of following formula

$$E_n(x) = (x + n) \mod 26.$$

$$D_n(x) = (x - n) \mod 26.$$

Now

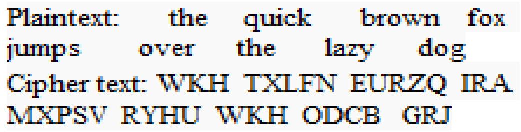
A=0,B=1,....,Z=25



Plain:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:
DEFGHIJKLMNOPQRSTUVWXYZABC

Above code is the example , when we take key of 3

While encoding, an individual investigates each letter of the message in the "plain" line and records the looking at letter in the "figure" line. Unwinding is done in reverse.



Plaintext: the quick brown fox jumps over the lazy dog
Cipher text: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

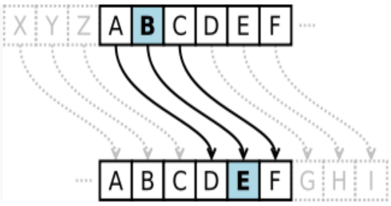


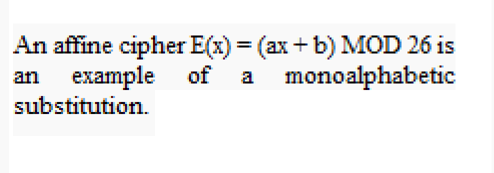
Fig. 3. Structure of Substitution Cipher

The working of the above figure is to supplant each plaintext letter with one a affirmed number of spots down the letter set. This model is with a move of three, so a B in the first information progresses toward becoming E in the figure content[4].

2. MONOALPHABETIC CIPHERS

In this method every commonness of a original data symbol is supplanted by a comparing figure content symbol to create figure content..

Example:

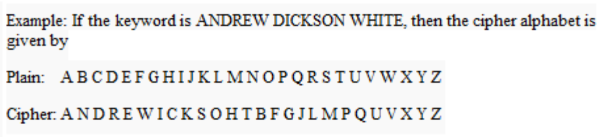


An affine cipher E(x) = (ax + b) MOD 26 is an example of a monoalphabetic substitution.

We have few more methods to create a monoalphabetic substitution.

Alphabet Mixing via a Keyword:

A catchphrase is to blend the letters to produce the figure letters in order.



Example: If the keyword is ANDREW DICKSON WHITE, then the cipher alphabet is given by

Plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher: A N D R E W I C K S O H T B F G J L M P Q U V X Y Z

Do you think it is a problem that there are 5 collisions (a plaintext letter being substituted for itself) in this substitution? (Answer: It depends.)

Perhaps a better keyword is EZRA CORNELL:

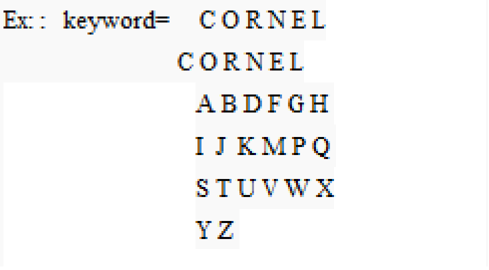
Plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher: E Z R A C O N L B D F G H I J K M P Q S T U V W X Y

Note that neither of these substitutions is generated by an affine cipher.

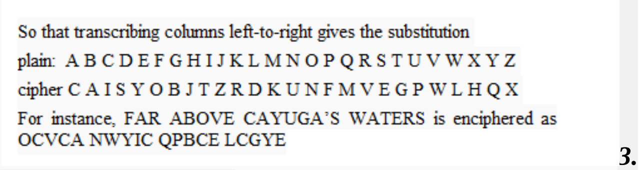
Alphabet Mixing via a Columnar Transposition:

The letters form the headings of the columns, and the left over letters of the alphabet fill in order in the rows below. Mixing is achieved by transcribing columns.



Ex: : keyword= CORNEL

```
CORNEL
 ABDFGH
 IJKMPQ
 STUVWX
 YZ
```



So that transcribing columns left-to-right gives the substitution

plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

cipher C A I S Y O B J T Z R D K U N F M V E G P W L H Q X

For instance, FAR ABOVE CAYUGA'S WATERS is enciphered as OCVCA NWYIC QPBCE LCGYE

3. PLAYFAIR CIPHER

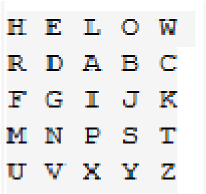
This method converts sets of letters (digraphs), rather than single letters just like the case with less difficult substitution figures, for example, the Caesar Cipher.

Recurrence examination is as yet conceivable on the Playfair method.

It applies and considers around 600 potential sets of letters rather than just 26 letters. Therefore the Playfair approach is extensively additional protected than more seasoned substitution approach.

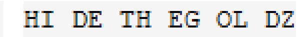
Main concept in this method is begins with making a key table. The key table is a 5×5 matrix of letters that will go about as the key for scrambling actual data. each one of the 25 letters must be strange additionally single letter of the letter set (typically Q) is discarded from the table (as there are 25 spots and 26 letters in the letter set).

Suppose we need to use the expression "Hello World" as our key. The beginning characters in the table will be the articulation, with duplicate letters cleared. The rest of the table will be stacked up with the remainder of the letters of the letter set, all together. Our key table would take after this:



H	E	L	O	W
R	D	A	B	C
F	G	I	J	K
M	N	P	S	T
U	V	X	Y	Z

Here, the message is part into digraphs, sets of two letters. On the off chance that there is an odd number of letters, a Z is added to the last letter. Suppose we need to encode the message "hides the gold".

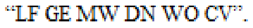


HI DE TH EG OL DZ

In encrypting procedure, The Playfair figure utilize a couple of basic standards identifying with where the letters of every digraph are in connection to one another. The guidelines are:

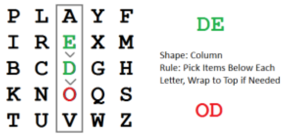
- On the off chance that the two letters are in a similar column, take the letter below each one (going back to the top if at the bottom)
- On the off chance that the two letters are in the comparative column, take the letter to one side of every one (returning to one side if at the most remote right)
- unless single or many of the preceding two rules are right , prepare a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle

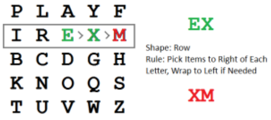
Using these rules, "hides the gold" with the key of "hello world" will be

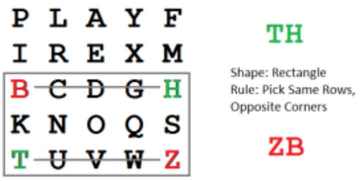


"LF GE MW DN WO CV".

This can be a slight tough to understand at first, but once it's comprehended it appears exceptionally quick and, generally, it is. Here's a visual case of each (contribution to green and coming about digraph in red):




P L A Y F
I R E X M
B C D G H
K N O Q S
T U V W Z
EX
Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed
XM



The Playfair cipher was utilized for the most part to ensure significant, yet non-basic mysteries, as it rushes to utilize and requires no uncommon gear. By the time enemy cryptanalysts could break the code the information it was protecting would often no longer be relevant.

4. HILL CIPHER

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra.

Each and every letter is denoted by a number modulo 26. frequently , this is simple method and will be is used

Retrieval Number: B14750982S1119/2019©BEIESP
DOI: 10.35940/ijrte.B1475.0982S1119

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

A=0,B=1,....,Z=25

,

be that as it may, this isn't a fundamental component of the figure. To secure a data, each group of n letters (considered as an n-component vector) is multiply by an *invertible* $n \times n$ matrix, against modulus 26. Reverse process will be used for getting actual data back.

The matrix used for encryption is the cipher key, also, it ought to be picked haphazardly from the arrangement of invertible $n \times n$ matrices (modulo 26). The figure can, obviously, be adjusted to a letter set with any number of letters; all math simply should be done modulo the quantity of letters rather than modulo 26.

Consider the message 'ACT', and the key below (or GYBNQKURP in letters):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Along these lines the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which relates to a figure content of 'POH'. Presently, assume that our message is rather 'CAT', or:

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

which belongs to a cipher text of 'FIN'. Every letter has altered. The Hill figure has accomplished Shannon's dissemination, and a n-dimensional Hill figure can diffuse completely crosswise over n symbols on the double.

DECRYPTION:

So as to decode, we convert the figure content once again into a vector, at that point just duplicate by the backwards framework of the key grid (IFKVIVVMI in letters).

We find that, modulo 26, the inverse of the matrix used in the previous example is

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \pmod{26}$$

Taking the previous example cipher text of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

this comes back to 'ACT', just as we hoped.

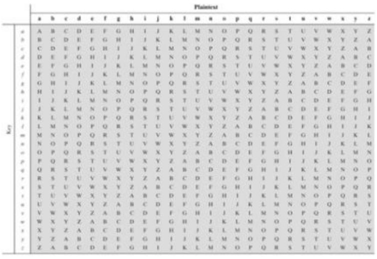
We have not yet examined two difficulties that exist in picking the scrambling grid. Not all cross sections have a regressive. The grid will have an opposite if and just if its determinant isn't zero. Moreover, by virtue of the Hill Cipher, the determinant of the encoding structure must not have any customary segments with the specific base.

5. POLY ALPHABETIC CIPHER

In this method, several cipher letters are used. classically the 26 × 26 grid, so that 26 cipher data alphabets are accessible. The system for filling the scene, and of picking which letters so as to utilize straightaway, portrays the particular poly alphabetic figure. Each such figure is more straightforward to break than were acknowledged since the substitution letter sets are repeated for sufficiently colossal plaintexts. One of the most predominant was that of Vigenere figure[8].

In this method, the starting line of the table rounded out with a duplicate of the plaintext letters in order, and progressive lines are essentially moved one spot to one side. A keyword i is then used to pick which cipher content letter set to utilize. Each letter of the keyword is utilized thus, and after that they are rehashed from the earliest starting point. So if the word is 'DOG', the first letter of word is enciphered with letter 'D', the second letter under 'O', the third letter under 'G', the fourth letter under 'D' again, and so on.

IV. RESULTS



		Plaintext																									
		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Key	a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 4. 26×26 Vigenere tableaux

Example:

1. The encipherer chooses a plaintext: VIGENERE

2. The encipherer picks a catchphrase and rehashes it to turn into the length of the plaintext, for example the catchphrase , "CIPH": CIPHCIPH

3. To encipher letter L1 of the original data, the encipherer makes another letter set wherein An is moved to letter L1 of the figure content, B is moved to the following letter, and so on.:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
CDEFGHIJKLMNOPQRSTUVWXYZAB

4. The encipherer finds the letters that compares to L1 in the substitution letter set. This is presently L1 of the plaintext: V⇒ X

5. This is rehashed for each letter in the plaintext and its relating letter in the key: VIGENERE + CIPHCIPH ⇒ XQVLPMGL

V. CONCLUSION

Cloud Computing is as yet another and developing worldview where registering is viewed as on-request administration. When the client takes the choice to move the information to the cloud, it loses authority over the information. Along these lines, in our proposed work, just the approved client can get to the information. Even if some intruder (unauthorized user) or service provider captures the data intentionally, he can't decrypt it and get back the original data from it. Here, we have scrutinized some important and mostly useful aspects of various substitution techniques to enhance data security.

REFERENCES

[1]. Kashish Goyal, Supriya Kinger, "Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975-8887), Volume 73-No.3,July 2013.

[2]. Abhuday Tirupathi, Parul Yadav, "Enhancing Security of Cloud Computing using Elliptic Curve Cryptography" International Journal of Computer Applications (0975 – 8887) Volume 57– No.1, November 2012

[3]. Priyanka Nema, Prof.Ashish Jain, "A Comparative Survey on Various Encryption Techniques for Information Security", International Journal of Social Sciences Volume-1, Issue-1, December-2013

[4]. Mohammed A. AlZain , Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 2012 45th Hawaii International Conference on System Sciences.

[5]. Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues"

[6]. Meiko Jensen, J¨org Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing.

[7]. Hassan Takabi and James B.D. Joshi, Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments"

[8]. Liang Yan, Chunming Rong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography"

AUTHORS PROFILE

P.Rajashekar, Asst.Professor at Department of CSE,VJIT,Hyderabad,Telangana India. He is currently pursuing Ph.D. from GITAM university He has published 5 papers in international journals.

Dr Aruna Kumari Professor at Department of CSE,VJIT, Hyderabad, Telangana India. She is Fellow of CSI(FCSI) , and Fellow of IEEE (FIEEE). She is DST Young Scientist Awardee (Govt. of India). She has more than 70 research articles in International Journals and Conferences.

PKVS Sarma,Asst.Professor at Department of CSE,VJIT,Hyderabad,Telangana India. He has published 4 Papers in international journals

Y Prabhu Kumar Department of CSE,VJIT,Hyderabad. He is currently pursuing Ph.D. from KL university, His research interest areas Data Mining, and Big Data