IJCSN International Journal of Computer Science and Network, Volume 5, Issue 4, August 2016
ISSN (Online): 2277-5420 www.IJCSN.org
Impact Factor: 1.02

A Novel Approach to Design Hybrid Vigenere Caesar Cipher Encryption with Genetic Algorithm (HVCEGA) for Data Security in Cloud Computing

[1] Sonal Pawar, [2] Dr. K. James Mathai

[1] M.Tech. Scholar, Dept. of Computer Engineering &Applications
NITTTR, Bhopal, India

[2] Associate Professor, Dept. of Computer Engineering & Applications
NITTTR, Bhopal, India

Abstract - In present scenario cloud computing is a large pool of easily and accessible virtualized resources, such as hardware, development platforms and software services. Cloud computing is a broad solution that delivers IT as a service. Cloud is an internet based technology which uses the Internet& central remote servers to support data and applications. In cloud computing, the data will be stored in data storage provided by cloud service providers. But still many business companies are not willing to adopt cloud computing technology due to lack of proper security control policy which lead to many vulnerability in cloud computing. Cryptography is mostly used technology to protect data within cloud environment. It is an art and science of hiding existing data from the external environment. It allows information to be sent in a secure form in such a manner that only authorized person is able to retrieve the original information. The paper presents a secure cloud data encryption technology which encrypts the data using Hybrid Algorithm (Vigenere and Caesar Cipher Encryption Algorithm and Genetic Algorithm- HVCEGA). A hybrid approach of more than one technique is more reliable and strong enough to provide security of data while processing and storage by using secured non-repeatable key (generated by one time pad). Computation time, avalanche effect and throughput are the parameters for which performance has been compared with existing encryption approach. The proposed HVCEGA algorithm provides more security by multi-layer encryption and reduces computation complexity using genetic algorithm.

Keywords - *Cloud Computing, Cryptography, Hybrid Algorithm, Genetic Algorithm, One Time Pad (OTP), Avalanche Effect.*

1. Introduction

Cloud computing is an important area in the field of networking which plays a vital role in internetworking. Now a day cloud computing is used in many areas like military, medical, industry etc. Cloud computing have some challenges in its use. Data security and privacy are some challenges; security is an important factor which affects the cloud computing technology, different security algorithm have been developed by different researchers to provide more security[9].

Cryptography algorithm provides a way to ensure data confidentiality and integrity. The data is always encrypted in the cloud then control is not lost. It is unconditionally secure if it is unbreakable even when the cryptanalysts has unlimited computational power and time[5]. The proposed HVCEGA algorithm use vigenere,Caesar cipher and genetic algorithm. Caesar cipher encryption algorithm use ASCII printable range from 97-122 and then convert the plain text into the Caesar cipher text by using custom key with it[14].Enhanced Vigenere encryption algorithm uses the defined square matrix termed as tabula recta, vigenere table and non-repeatable key(generated by one time pad) to encrypt the plain text. One Time Pad(OTP) is truly random key is used for only one time whose length is equal to the plain text length. Shannon proved that this system provide perfect secrecy.Genetic Algorithm (GA) has proven to be reliable and powerful optimization technique in variety of application. It can be applied to both texts and images. GA is secure since it does not utilize the natural number directly. Ensure confidentiality and added security in network reduces computation complexity[3].

2. Related Work

Nandita Sen Gupta and Jeffrey Holmes [1],have discussed the designing of cryptography based security system for

cloud computing. Authors have proposed an efficient hybrid cryptography system named as Hybrid Vigenere Caesar Cipher Encryption (HVCCE). The HVCCE will prevent the cloud infrastructure in three main places: in client location, in the network and in server. HVCCE has three phases in the first phase Caesar cipher is applied on the plain text, in the second phases according to vigenere square value, vigenere cipher is applied along with the keyword on the encrypted text achieved from the first phase. In the third phase according to vigenere square value, vigenere cipher is applied with the reverse word of the keyword considered in second phase. This encryption is applied on the encrypted text achieved from second phase. Similarly decryption is to be done in three phase in reverse process. Author said that this cryptographic security system is designed in such a way that computation time for decryption of cipher text message for the hackers will be more as compared to any single cryptographic system.

Gagan Singh and Supriya[2], have modified vigenere encryption algorithm. Its hybrid implementation with base 64 and AES has proposed a hybrid approach for applying encryption algorithms different kind of algorithm such as substitution cipher, symmetric algorithms etc. are used. The system security is greatly improved through researching several famous data encryption algorithms (vigenere encryption algorithm, base 64, AES) and improving these data encryption algorithm and arranging in a suitable order. Avalanche effect is chosen as a metric for measuring performance of proposed algorithm shows significant high avalanche effect, as compare with vigenere encryption algorithm author conclude that single encryption algorithm do not provide enough security to cope up with today's security demands modified vigenere encryption algorithm (MVEA), base 64, AES algorithm to improve the security of data.

Sindhuja K and Pramela Devi [3], in their paper have discussed on symmetric key encryption technique using genetic algorithm key have proposed a genetic algorithm based symmetric key cryptosystem for encryption and decryption. Here the plain text and the user input are converted into text matrix and key matrix respectively. An additive matrix is generated by adding the text matrix and key matrix. A linear substitution function is applied on an additive matrix to produce the intermediate cipher. Then the generic algorithm (GA) functions (crossover and mutation) are applied on the intermediate cipher to produce the final cipher text. GA is secure since it does not utilize the natural numbers directly. In their paper author use two point crossover techniques and flipping of bits mutation technique. Author stated that symmetric key substitution algorithm is used to ensure confidentiality in networks which is combined and implemented with the help of genetic algorithm function to provide added security.

2.1 Problem Identification

In cloud computing security is an important factor which effects the data transmission. A single encryption algorithm of cryptography techniques is not sufficient to provide security of data over cloud. Normal transmission of original data in same form is unsafe. So there is need of some efficient security algorithms for data transmission in cloud computing. In cryptography based architecture design of security algorithm which provides secure and efficient data transmission to increase security and privacy is affected by many parameters such as computation time, key size, throughput, encryption level. Different research has been done by different researchers for designing the security algorithm using different encryption algorithm for cloud computing to provide security. In the research work proposed by N. Sengupta and J. Holmes [1] for data transmission researchers have selected two encryption algorithms together to provide security of data by encrypting it with both encryptions.

3. Proposed Work

The proposed HVCEGA algorithm use modified vigenere Caesar cipher encryption to secure data with multi-layer encryption which uses One Time Pad (OTP) to generate random key and reduce computation complexity by genetic algorithm.

In this hybrid algorithm enhanced vigenere cipher algorithm is used which is more efficient as compared to the existing algorithm and OTP is used to generate random key for encryption which is not repeated. It also used to provide more layer of security data will also encrypted by genetic algorithm functions. After encrypting by three algorithms final encryption cipher is ready to transmit or store over cloud.

3.1 Block Diagram Of Proposed Hvcega Algorithm

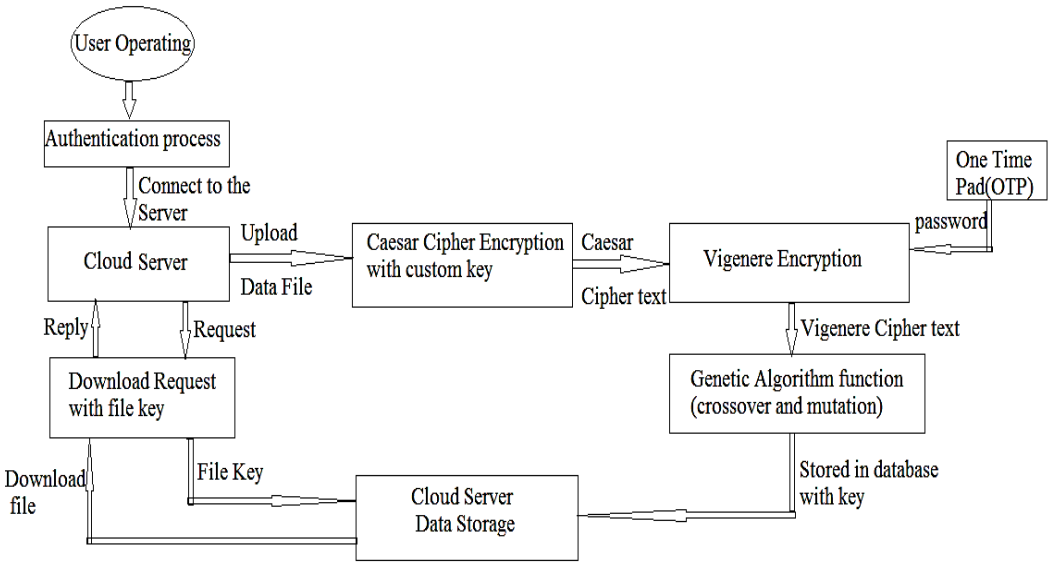


Fig1: Block Diagram of Proposed HVCEGA algorithm

When user enters the plain text then at server side, the plain text is converted into encrypted text by using hybrid encryption algorithm, in which different keys are used. In Caesar cipher encryption plain text is computed with custom key for encryption and then Caesar cipher text is encrypted by vigenere cipher encryption using OTP generated key. Then vigenere cipher text is again encrypted by Genetic Algorithm (GA) functions, to generate its final cipher text to be stored in the cloud.

4. Implementation

The proposed hybrid algorithm was successfully implemented in cloudsim with an environment Windows 8 home basic (64-bit) operating system, Intel Core i3-2330M processor 2.20 GHz clock rate, and memory of 4GB RAM, 1 GB hard disk. Research tools Used-Jdk8 Updated Version, Cloud Simulator API, Net beans IDE [7] and My SQL.

4.1 Flow Diagram

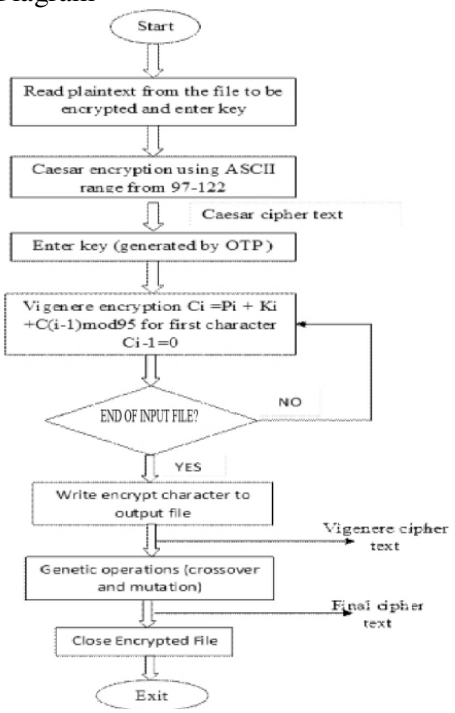


Fig. 2: Flow diagram of HVCEGA

The steps for design the HVCEGA are as follow:

Step 1: To encrypt the data, user enters the plain text.

Step 2: Caesar cipher encryption- encrypt the text with custom key generated by user and generate Caesar cipher.

Step 3: After that Caesar cipher text is encrypted with vigenere encryption. For vigenere encryption the key is generated by One Time Pad (OTP) and then compute with Caesar cipher and generate vigenere cipher text.

Step 4: Vigenere cipher is encrypted by genetic algorithm functions.

Step 4.1 Crossover function

Step 4.2 Mutation function

Step 5: Final encrypted cipher text is stored in database of cloud with key.

Step 6: Decryption of the data file is similar to the encrypted cipher text. It is decrypting in the reverse process of encryption i.e. from follow the steps 5 to step 1.

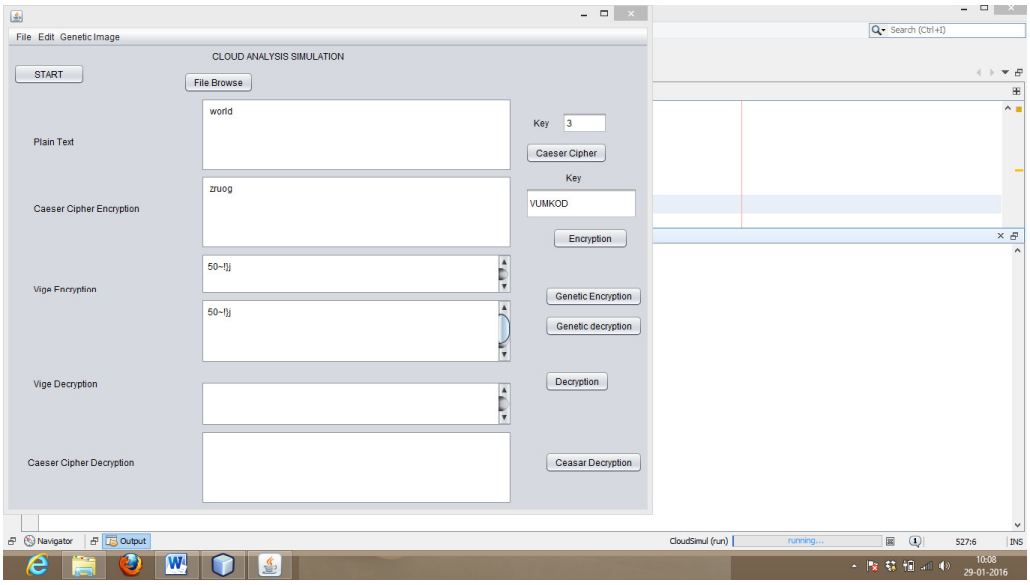


Figure 3: Screen Shot: HVCEGA algorithm simulate in cloudsim using netbeans

Cloudsim [6] simulate Hybrid Vigenere Caesar Cipher Encryption with Genetic Algorithm (HVCEGA) and GUI application support source code of algorithm. The above figure 3 shows that how the encryption algorithm is work in cloudsim simulator. The plaintext is encrypted by each algorithm in a sequence and then the final cipher text is stored in cloud.

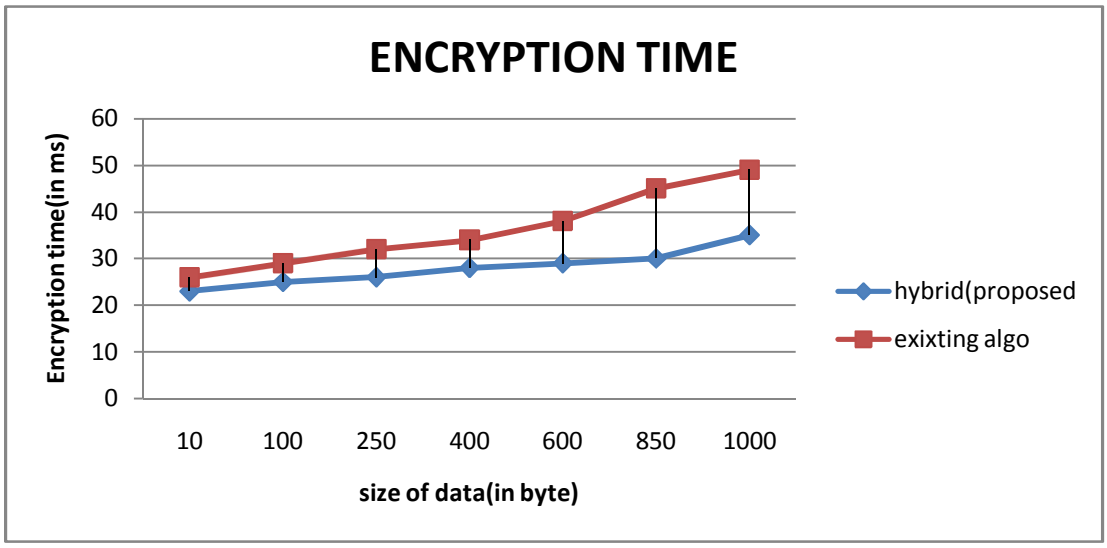
5. Result

Researcher have successfully simulated the concept of enhanced hybrid algorithm using GA functions method through cloudsim and analysed the result. Computation time, avalanche effect and throughput are the parameters for which performance of proposed HVCEGA (Hybrid Vigenere Caesar Cipher Encryption with Genetic Algorithm) algorithm has been compared with existing HVCCE (Hybrid Vigenere Caesar Cipher Encryption) algorithm using seven different filesizes of data.

5.1 Encryption Time

For calculating the computation time taken for data encryption by the algorithm seven different size files are used by existing HVCCE algorithm and proposed HVCEGA algorithm. All seven files are encrypted by both algorithm and the times taken by each algorithm to encrypt the files are compared.

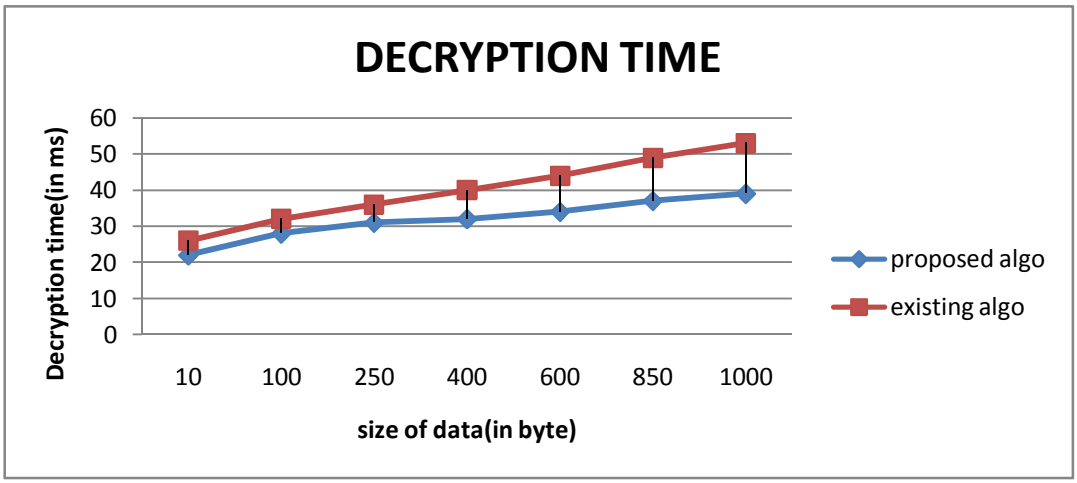
It can be analysed from above Graph 1 that as the encryption time by HVCEGA is less as compare to HVCCE algorithm used for data encryption concept.



Graph 1: Computation of data encryption time HVCCE visa-a-viz HVCEGA algorithm

5.2 Decryption Time

For the computation of decryption time for data decryption in the algorithm all same seven files are decrypted by existing HVCCE and proposed HVCEGA algorithm and the decryption time is calculated.



Graph 2: Representation of Decryption Time HVCCE visa-a-viz HVCEGA Algorithm

It can be analysed from both graph 1 and 2 that Proposed (HVCEGA) algorithm takes less time for encryption and decryption.

5.3 Avalanche Effect

Avalanche effect refers to an enviable property of cryptographic algorithm where, if an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g. more than half the output bits flip) [18]. In this section, researcher has compared HVCEGA and HVCCE taking Avalanche effect as a performance metric. Researcher took "COMPUTING" as plaintext and "KEYWORD" as key for all cases to obtain the results.

Case I: Changed middle character of plaintext: On flipping one bit of middle character from the plain text, we

get "COMPETING" (on flipping U (01010101) to E (01000101)).

Table 1: Changed middle character of plaintext

	ENCRYPTION TECHNIQUES	
	EXISTING ALGORITHM(HVCCE)	**PROPOSED ALGORITHM(HVCEGA)**
PLAIN TEXT	COMPUTING	COMPUTING
PASSWORD	KEYWORD	KEYWORD
CIPHER TEXT	PUNOLNOAN	DSA;DZK
MODIFIED TEXT	COMPETING	COMPETING
MODIFIED CIPHER TEXT	PVNOVNOAN	@FCRAB/
NO. OF BITS FLIPPED	8	14
AVALANCHE EFFECT	12.5%	21.39%

Table1showshigh avalanche effect of HVCEGA as compared with HVCCE when only the middle character of plain text is flipped.

Case II: Changed middle character of password: On flipping one bit of middle character from password, we get "KEYRORD" (on flipping W (01010111) to R (01000111)).

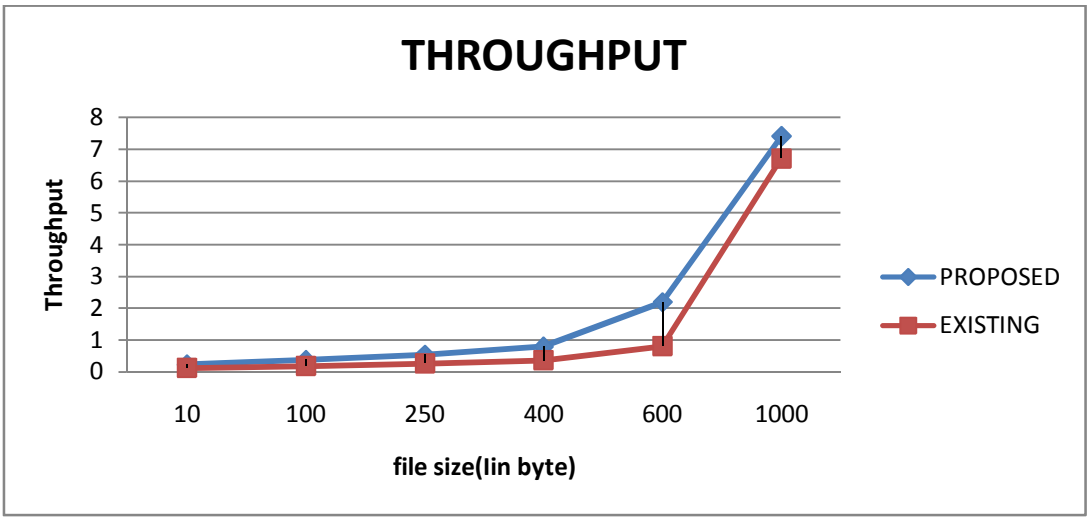
Table 2: Changed middle character of password

	ENCRYPTION TECHNIQUES	
	EXISTING ALGORITHM(HVCCE)	**PROPOSED ALGORITHM(HVCEGA)**
PLAIN TEXT	COMPUTING	COMPUTING
PASSWORD	KEYWORD	KEYWORD
CIPHER TEXT	PVNOLNOAN	DSA;DZK
MODIFIED PASSWORD	KEYRORD	KEYRORD
MODIFIED CIPHER TEXT	PVNJLNOAN	6GAGWZD
NO. OF BITS FLIPPED	6	10
AVALANCHE EFFECT	8.33%	14.2%

The Table 2 shows high avalanche effect of HVCEGA as compared with HVCCE. From table 1 and 2 it clearly shows that the proposed (HVCEGA) algorithm has more avalanche effect as compare to the existing (HVCCE) algorithm

5.4 Throughputs

Throughput is a measure of how many data an algorithm can encrypt in a given amount of time. For calculating the throughput for data encryption by the algorithm seven different size files are used by existing HVCCE algorithm and proposed HVCEGA algorithm.



Graph 3: Throughputs of HVCEGA algorithm and HVCCE algorithm

Throughput of encryption algorithm is calculated by data size and the total computation time. Above Graph 3 shows that the throughput of proposed HVCEGA algorithm is more than the existing HVCCE algorithm that shows that the proposed HVCEGA algorithm is more efficient and feasible as compare to existing HVCCE algorithm.

6 Conclusion and Future Work

In this paper hybrid algorithm is used for multi-layer encryptions which provide higher security. The main advantages of hybrid algorithm is that multiple encryption algorithm are used which is more secure and it reduces computation complexity by using GA functions. The comparison shows that HVCEGA algorithm reduces the computation time and avalanche effect is high as compare to HVCCE algorithm and also provides better security against brute force attack and data modification attacks. And throughput is increased as compare to the existing HVCCE algorithm. In future the performance of HVCEGA algorithm can be tested in real time environment and a possibility is to use the HVCEGA algorithm for video files in cloud computing for encryption.

References/Bibliography

[1] N. Sengupta and J. Holmes, "Designing of Cryptography Based Security System for Cloud Computing", In Cloud Ubiquitous Computing Emerging Technologies (Cube), International Conference, 2013.

[2] G. Singh "Modified Vigenere Encryption Algorithm and its Hybrid Implementation withBase64 and Aes", In Advanced Computing, Networking and Security (Adcons), 2nd International Conference On, 2013.

[3] K. Sindhuja and S. Pramela Devi, "A Symmetric Key Encryption Technique Using Genetic Algorithm",Int J ComputSci Inform.Tech., Vol. 5, No. 1, Pp. 414-6, 2014.

[4] G. Vijay and A. R. M. Reddy, "An Efficient Security Model in Cloud Computing Based on Soft Computing Techniques",International Journal of Computer Applications, Vol. 60, No. 14, 2012.

[5] William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice-Hall - Pp.80- 81.

[6] Cloud simulator Http://Cloudbus.Org>Cloudsim.

[7] Java downloads Www.Netbeans.Org.

[8] Kinamik, "The CIA Triad: Have You Thought About Integrity", Kinamik Data Integrity, 2007.

[9] Peter Melland Tim Grance, "The NIST Definition of Cloud Computing", NIST, 2010.

[10] Cloud Computing Principles, Systems and Applications Nick Antonopoulos Http://Mgitech.Wordpress.Com.

[11] Cloud Computing Methodology, Systems and Applications Lizhe Wang, Rajiv Ranjan. Http://Www.Unitiv.Com.

[12] Ajit Singh, AartiNandal and Swati Malik, "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security", International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 12. Pp. 78-82, December 2012.

[13] Quist-AphetsiKester, "A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher," Ghana Technology University College, Accra North, Ghana, January 2013.

[14] Dr.Fadhil Salman Abed, "A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganogrpahy", Ijaiem - Issn 2319 – 4847, Volume 2, Issue 4,april 2013.