MANTECH Publications
Journal of Digital Image Processing and Computer Vision
Volume 3 Issue 3

Securing data in Cloud Storage with Advanced Cloud Security using Symmetric Encryption Algorithm

Harpinder Singh[1], Sheetal Kalra[2], Sarabpreet Singh[3]
Assistant Professor[1, 2, 3]
Department of CSE
ACET, Amritsar, Punjab, India [1, 3], GNDU, RC, Jalandhar, Punjab, India[2]
Correspondence Author's E-mail: *harpinder2065@gmail.com*

Abstract

Cloud computing is still in its infancy in spite of gaining tremendous momentum recently. High security is one of the major obstacles for opening up the new era of the computing as a utility. As the sensitive applications and data are moved into the cloud data centers to runs on virtual computing resources in the form of virtual machine. It might be difficult to track data security issues in cloud computing environment. So this paper aims to highlights the main privacy, security and trust issues in cloud computing. In this manuscript it presents some existing classical encryption techniques for securing the data in cloud. This paper also proposes encryption decryption algorithms to address the security and privacy issue in cloud storage in order to protection on data in the cloud computing.

Keywords*: - Cloud storage, Symmetric encryption, Data security*

INTRODUCTION

Cloud computing is a service that can store data on server remotely using internet. The main advantage of cloud is reducing cost by sharing storage resources, combined with an on demand service provision mechanism relying on a pay-per-use model [1]. These features have a direct affect on traditional security, privacy and trust mechanisms. It can become disadvantage of maintain a level of sufficient to sustain confidence in customers. Cloud security and privacy concerns are arising in which both customer's data and application are residing in provider's premises. Security and privacy are always a major concern in cloud computing as shown in Fig.1. It shows the survey report of 2009 by

International Data Corporation (IDC) [17]. From the figure, it is clear that security is the top most concern in cloud computing in the survey of the year. There are multiple security challenges in cloud computing. These challenges relate to cloud server having physical control of data, relate to identity and credential management, relate to data verification, tempering, integrity, confidentiality, data loss and theft.

To protect private and sensitive data that are processed in data centers, the cloud user needs to verify (a) the real exists of the cloud computing environment in the world; (b) the security of information in the cloud; and (c) the trustworthiness of the systems in cloud computing environment. However, the management of data and services are not secure and trustworthy in cloud data centers. Some core mechanisms for addressing privacy (as model contracts) are no longer trustable, flexible or dynamic enough, so new technique need to be developed to fit this paradigm. The cryptography provide data encryption, in any form of usage it can prevent potential data leakage that is particularly critical in a cloud computing environment [13].

This paper provides some issues in data security and based on these issues we provide hybrid symmetric encryption technique to secure the data in cloud environment. Our contributions of this paper are organized as follows. In section second, survey the most relevant privacy, security and trust issues that pose threats in current existing cloud computing environments. In section third, analyses the issues of cloud data storage. In section four and five present encryption technique that may be addressed to eliminate these potential security, privacy and trust threats, and providing a high secure, trustworthy, and dependable cloud computing environment. In section sixth, proposed new encryption technique to secure the data. Finally, conclusions and a direction for future work are given in section seventh.

RELATED WORK

In Zhou [3], the authors discuss the cloud security issues of availability, confidentiality, data integrity, control and audit in addition to privacy issues. There is a significant discussion of how various CSPs are meeting the security challenges of the various areas, especially for the areas of availability, confidentiality, data integrity and control. The discussion of auditing challenges is more general. The

authors advocate for auditing to take place in a software layer within the virtual operating system and that such a system should provide minimal-over head monitoring of events and logs.

Mackay [4] this paper presents a concept for an innovative integrated platform to reinforce the integrity and security of cloud services and context of critical Infrastructures to identify the core requirements, components and features of this infrastructure.

Dawei Sun[2] This paper primarily aims to highlight the major security, privacy and trust issues in current existing cloud computing environments and help users recognize the tangible and intangible threats associated with their uses, paper cover two main aspects of security, privacy and trust issues, which include: (a) surveying the most relevant privacy, security and trust issues that pose threats in current existing cloud computing environments, and (b) analyzing the way that may be addressed to eliminate these potential security, privacy and trust threats, and providing a high secure, trustworthy, and dependable cloud computing environment.

Juraj Somorovsky [8] in this paper, author provided security analysis to the control interfaces of a large Public Cloud provider (Amazon) and widely used software of Private Cloud provider (Eucalyptus). The research results are in regards to the Amazon EC2 and S3 services, the control interface could be compromised via the advanced XSS techniques and novel signature wrapping technique.

Diaa Salama [13] this paper provides evaluation of six of the most common encryption algorithms namely: AES (Rijndael), Blowfish, DES, 3DES, RC2 and RC6 Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Encryption algorithms play a main role in information security systems. On the other side, those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power.

ISSUES IN CLOUD DATA STORAGE

Trust, Security and Privacy are on-going research issues in any development, as new security holes will appear with hackers advancing in their efforts [14][18]. There are some issues in data storage of cloud.

Security

Security is one of the most obstacles for opening up the new era of computing as a utility. Security is the absence of unauthorized access to, or handling of, the system state [5]. The main dimensions of security are availability, confidentiality and integrity. Security issues in cloud computing environments can be divided into some sub-categories which include: (a) how to provide safety mechanisms, so that to monitor or trace the cloud server, (b) how to keep data confidentiality for all the individual and sensitive information, (c) how to avoid service hijacking, where phishing, fraud and exploitation are well known issues in IT,(d) how to avoid malicious insiders illegal operation under the general lack of transparency into provider process and procedure environments, (e) how to develop appropriate law and implement legal jurisdiction, so that users have a chain against their providers if need.

Privacy

Cloud computing utilizes the virtual computing technology [14]. User's personal data may be scattered in various virtual data centre rather than stay in the same physical location. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depending on the computing task submitted by the users. according to cloud scenario, the privacy issues differ and can be divided into categories (a) how to users remain control over their data in cloud when data is stored and processed, and avoid nefarious use, theft and unauthorized resale, (b) which party is responsible for ensure legal requirements for personal information. (c) How to guarantee data replications and consistent state, where replicating data to multiple prefer locations is a usually choice, and avoids data leakage and unauthorized fabrication.

Trust

Trust is viewed as a measurable belief that utilizes experience, to make trustworthy decisions [2]. To protect clouds, traditional hard security techniques such as authentication and authorization provide a solid foundation, but they fail when cooperating entities act maliciously due to scale and temporary nature of collaborations. Trust as a soft social security philosophy can fight against such security threats by restricting malicious entities from participating in interactions and consequently offers a high trustworthiness cloud computing environment [14]. Trust issues in cloud computing environments can be divided

into sub-categories, which include: (a) how to definition and evaluation trust according to the unique attribute of cloud computing environments, (b) how to handle malicious recommend information, which is very important in cloud computing environments, as trust relationship in clouds is temporary and dynamic, (c) how to consider and provide difference security level of service according to the trust degree, (d) how to manage trust degree change with interaction time and context, and to monitor, adjust, and really reflect trust relationship dynamic change with time and space

Performance

Business organizations are worried about acceptable levels of performance and availability of applications hosted in the cloud. Application and data in the cloud storage should be available to the users at anytime and anywhere. Users have no worry about the local system which is used for accessing the cloud servers.

Ownership

Once data has been submitted to the cloud, developers have concern about losing their rights or being unable to be protecting the rights of customers. Many cloud providers address this issue with well-skilled user-sided agreements. According to the agreement, users would be wise to seek advice from their favorite legal representative.

Long-term Viability

Users should be sure that the data put into the cloud will never become invalid even the cloud computing provider get lost or get acquired and swallowed up by a larger company. Users should ask their potential providers of cloud how they would get users data back and if it would be in a format that user could import into a replacement application.

Data Portability and Conversion

Users have concerns on data portability like, switching between service providers. There may be difficulty in transferring data. Converting and porting data is highly dependent on the cloud provider's data retrieval format, particularly in case where the format cannot be easily revealed. As service competition grows, open standard become established and the data portability issue will ease and supporting the more popular cloud providers conversion processes will become available. Worst case is that the cloud subscribers have to pays for custom data conversion. These are certain areas in which cloud computing requires to excel and solve problem related

to it. Out of all the problems; narrated Security and Privacy put the major threats in growth of cloud computing. It needs to be worked upon.

Data Backup

The traditional backup methods used with applications and data centers that were designed for consumer and web applications. In case of disasters the Software as a service vendor needs to ensure that all sensitive data is regularly backed to facilitate quick recovery. Also it use of strong encryption method to protect the backup data is recommended to prevent accidental leakage of sensitive data.

Symmetric Encryption

Symmetric encryption technique involves the use of a single secret key for both the encryption of data and decryption of data.

Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data [9]. For example, a source produces data in plaintext, A = [A1, A2, A3….Am]. For Encryption, a key is generated at the data source. Then the key is provided to the destination by means of some secure channels. Data A and the key K as input, the encryption algorithm forms the cipher text C = [C1, C2….Cn]. This may be written as C=E_K (A). Cipher text C is produced by using encryption algorithm, where E indicates the encryption algorithm used and K indicates the key used for encryption. At the receiver end, receiver should apply decryption algorithm with same secret key used for encryption to get the actual dataA=D_K (C).Here D indicates decryption algorithm.

Classical Encryption

Two building blocks of all classical encryption techniques are substitution and transposition [12]. In substitution, replace elements of the plaintext with elements of cipher text and in transposition rearranging the order of appearance of the elements of the plaintext. Permutation is also referred to as transposition.

Caesar cipher

This is example of a substitution cipher method [6]. In Caesar cipher each character of a message is replaced by three positions down in the alphabet. This cipher can be broken by brute force attack.

Plaintext: ARE YOU READY
Cipher text: DUH BRX UHDGB

One can see that such a cipher may be difficult task to break. This cipher can be

broken by brute force attack because at the end there are only 25 possible options of key.

The Playfair cipher

Playfair cipher is example of classical sub stitution cipher which has a square matrix of 5x5 alphabetical letters arranged in an appropriate manner. The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 25*25=625 possible digraphs rather than the 25 possible monographs [16]. The user can select a key and place in the matrix order. The remaining letters of alphabet from the key are then one by one placed in the matrix of the Playfair cipher. The plain text is broken into the pairs if pairs has same letter alphabets then they are separated by a filler letter with 'x'. Otherwise if the pair is with different alphabetical letters and resides in matrix same row then every letter is replaced by the letter ahead. If the pair of letters is in the same column of matrix then each letters is replaced by the letters below it and when the pair of letters is neither in the same column and neither in the same row then they replaced by the letter in row that resides at the intersection of paired letters.

Vigenere cipher

Vigenere cipher when compared with Caesar cipher gives introduction of keywords with some level of security [15]. These keywords are repeated to cover the length of the plaintext which is to be encrypted form. The user send the data chooses a keyword and repeats it until it matches the length of the plaintext. For example: key "POL"

The first letter of the plaintext H is paired with P, the first letter of the key. So use row P and column H of the Vigenere square, namely W. Similarly, for the second letter of the plaintext, the second letter of the key is used the letter at row O and column E is S [10]. The rest of the plaintext is enciphered in a similar way:

Plaintext: HELLO
Key: POLPO
Cipher text: WSWAC

As it can be seen from that above example, "POL" is a keyword and plain text is "HELLO" which is encrypted into "WSWAC" [9]. This work through Vigenere table which contains alphabets in form of rows and columns. The left most column indicates keyword and top most row indicates plaintext and at the junction

of two alphabetical letters resides our replacement. After individually transforming every letter, user gets an encrypted message.

Rail Fence Technique

The rail fence cipher is also called a zigzag cipher. This is one of the transposition ciphers [7], in which the plain text is written down as a sequence of diagonal and then read as sequence of rows. For example, encipher the message "HOWAREYOU" with a rail fence of depth 2,

H W R Y U

O A E O

Now the encrypted message is "HWRYUOAEO". In this technique the same alphabets in the plaintext is rearranged [11]. This technique alone cannot be sufficient for data security.

Proposed work

Proposed technique emphasizes on improving classical encryption techniques by integrating substitution cipher and transposition cipher. Both substitution and transposition techniques have used alphabet for cipher text. In the proposed algorithm, initially the plain text is converted into corresponding ASCII code value of each alphabet. In classical encryption technique, the key value ranges between 1 to 26 and key may be string (combination alphabets). But in proposed algorithm, the key value range 1 to 256. This algorithm is used in order to encrypt the data of the user in the clouds. The user encrypts the data with proposed encryption method and sends this encrypted data into the cloud storage. The data are stored into the cloud as in encrypted form. Since the user has no control over the data after his session is logged out, the encryption key acts as the primary authentication for the user. Proposed algorithm is described below.

Encryption algorithm

1. Followings are the steps in proposed encryption algorithm.

2. Count the Number of characters N without space in the plaintext.

3. Convert the plaintext into equivalent ASCII code value and form a square matrix S*S >=N.

4. Apply converted ASCII code from left to right in the square matrix. After this divide the matrix into three parts namely upper matrix, diagonal matrix and lower matrix.

5. Read the value from left to right in each matrix.

6. Each matrix use three different key K=K1, K2, K3 for encryption. Do the encryption.

7. Apply the encrypted value into the matrix in the same order of upper, diagonal and lower series.

8. Read message by column by column in the table. Here the order in the columns read from the matrix is the key number K4.

9. Convert the ASCII code value data into equivalent character value.

The followings are the detailed description of each step in the proposed encryption algorithm.

Step 1:- Count the number of characters N in the data without space.

Plaintext - THISISSECRETDATA
N= 16 (N = Number of Characters in the Message)

Step 2:- Convert the plain text into equivalent ASCII code and form a square matrix.

ASCII code value for the plaintext:
84 72 73 83 73 83 83 69 67 82 69 84 68 65 84 65

To form a square matrix, choose a number (S), square value of S is immediately next to N. i.e. S2 is nearest square value N and S2 >= N. For this plaintext N=16, so S=4. The order of matrix is 4*4>=16, Form a 4*4 matrix.

Step 3:- Apply the converted ASCII code message row by row in S * S matrix. Separate the matrix into three parts as Upper, Diagonal and Lower. Following shapes represent the upper, diagonal and lower matrix position in the square matrix.

84	72	73	83
73	**83**	83	69
67	82	**69**	84
68	65	84	**65**

- Upper  - diagonal  -Lower 

Step 4:- Read the data from left to right for upper, diagonal and lower

84	72	73	83
73	**83**	83	69
67	82	**69**	84
68	65	84	**65**

The values of three matrixes are,

Upper matrix – 72 73 83 83 69 84

Diagonal matrix - 84 83 69 65

Lower matrix - 73 67 82 68 65 84

Step 5:- To encrypt the message use three different keys for upper, diagonal and lower matrix separately.

Keys are K=K1 for upper matrix, K2 for diagonal matrix and K3 for lower matrix.

Upper matrix =18 -- K1

Diagonal matrix =12 -- K2

Lower matrix = 5 -- K3

Now add this key value with ASCII code data of each matrix.

After Encryption:

Upper Matrix- 90 91 101 101 87 102

Diagonal Matrix- 96 95 81 77

Lower matrix- 78 72 87 73 70 89

Step 6:- Apply the data into the square matrix in the same order of how it was read.

96	90	91	101
78	**95**	101	87
72	87	**81**	102
73	70	89	**77**

Step 7:- Now Read the data from the matrix by column by column. Here the order of the columns read in the matrix is the key K4.

4 2 1 3 -----K4

96	90	91	101
78	95	101	87
72	87	81	102
73	70	89	77

The text is 91 101 81 89 90 95 87 70 101 87 102 77 96 78 72 73

Step 8:- Covert the ASCII code into the equivalent character value. Then,

Encrypted cipher text is [eQYZ_WFeWfM’NHI

Decryption Algorithm

The encrypted data is stored in the cloud storage. To retrieve the data from cloud, decryption is necessary to get the actual data from cloud.

Decryption is possible only with key values which are used for encryption. So key should have a vital role in encryption and decryption algorithm.

Following steps illustrate the decryption algorithm.

1. Convert encrypted text into ASCII code value.

2. Count the number of character N in the decrypted text and form a square matrix S*S.

3. Apply the ASCII code in the S*S matrix as column by column based on key K4.

4. Divide the matrix into upper, diagonal and lower order series.

5. Apply reversed encryption using the keys K1, K2 and K3 on the upper, diagonal and lower matrix order respectively.

6. Apply data into matrix table by upper, diagonal and lower matrix order.

7. Read the data as row by row from left to right in matrix.

8. Convert the ASCII code value into character value.

The followings are the detailed description of each step in the decryption algorithm.

Step1:- Each character in the encrypted text is converted into equivalent ASCII code values.

Encrypted cipher text is [eQYZ_WFeWfM'NHI

Convert it into ASCII code, as below

The text is= 91 101 81 89 90 95 87 70 101 87 102 77 96 78 72 73

Step2:- Count the No. of character (N) in the decrypted text and form a square matrix S*S. Number of characters are N=16, so S=4, Order of matrix is 4*4.

Step3:- Apply the ASCII code in the S*S matrix as column by column based on key K4.

96	90	91	101
78	95	101	87
72	87	81	102
73	70	89	77

Step4:- Divide the matrix into upper, diagonal and lower.

Read the message in the matrixes from left to right.

96	90	91	101
78	**95**	101	87
72	87	**81**	102
73	70	89	**77**

Upper Matrix - 90 91 101 101 87 102

Diagonal - 96 95 81 77

Lower matrix - 78 72 87 73 70 89

Step5:- Apply reverse encryption using the keys K1, K2 and K3 on the upper, diagonal and lower matrix respectively.

Upper matrix =18 ---- K1
Diagonal matrix =12 -- K2
Lower matrix = 5---- K3

Perform decryption using the keys. The values of three matrixes after decryption

Upper matrix – 72 73 83 83 69 84
Diagonal matrix - 84 83 69 65
Lower matrix - 73 67 82 68 65 84

Step6:- Apply the data into matrix by upper, diagonal and lower matrix.

84	72	73	83
73	**83**	83	69
67	82	**69**	84
68	65	84	**65**

Step7:- Read the data as row by row from left to right.
84 72 73 83 73 83 83 69 67 82 69 84 68 65 84 65

Step8:- Convert the ASCII code into equivalent character value.

Then, Decrypted result is,

Original Plaintext – THIS IS SECRET DATA

The original text is retrieved by the user after completion of all these steps in the decryption algorithm. Key is more important to perform encryption and decryption. This method is more secure the data because algorithm could be known to everyone but key should be known only to authorize users.

Algorithm analysis

In private key technique, only one key is used for encryption and decryption. In this technique, sender and receiver have already known about key before exchange information securely. Important advantages of private key technique are its security and high speed. Proposed encryption model is a new block cipher.

It has N number of rounds, and 256 bits-length secret key. The secret key will use to fill an expanded key table which is then used in encryption. Both differential and linear attacks on proposed encryption model will recover every bit of the expanded key table without any exhaustive search. However, the plaintext requirement is strongly dependent on the number of

rounds. For 256-bit block size, differential attack on proposed encryption model uses 245 chosen plaintext pairs (about the same as DES), while 262 pairs are needed for 12-round proposed encryption model. Thus, conclude that 12 rounds are sufficient to make differential and linear cryptanalysis of proposed encryption model impractical.

Advantages

The proposed encryption model offers some advantages are as follows. Proposed model will be fast, suitable and secure for encryption of large files. The proposed encryption model will simple to implement and will have complexity in determining the keys through crypto analysis. Another, the procedure will produces a strong avalanche effect making many bits in the output block of a cipher to undergo changes with one bit change in the secret key.

Some more advantages are listed below:

- Flexibility
- Reliability
- Highly Efficient
- Good Response Time
- Good Memory Utilization
- No complex architecture
- Good CPU Utilization

Results and calculation of avalanche Effect

From the results calculation it's analysed that we can increase performance parameters by using proposed encryption model as compare existing. Also, we can see that the classical ciphers like Playfair cipher, Vigenere Cipher, Caesar Cipher etc. have very less Avalanche Effect and hence cannot be used for encryption of confidential messages.

$$f(x) = \frac{1}{2^n} \sum_{fn}^{n} W(a_j^n) \quad \text{.....(1)}$$

$$W(a_j^n) = = \sum_{f=1}^{n} a_j^n \quad \text{all X} = \{0,1\}^n \quad \text{..... (2)}$$

2^n In range $0 \leq W(a_j^n) \leq 2^n$

$$K_{avalanche}(t) = \frac{1}{n^{2^n}} \sum_{f=1}^{n} w\left(a_j^n\right) = \frac{1}{2} \quad \text{..... (3)}$$

The modern encryption techniques are better than classical ciphers as they have higher Avalanche Effect.

Avalanche effect can be calculated by using equation.

Avalanche Effect (%) = (Number of Changed Bits in Cipher text) / (Total number of bits in cipher text) * 100.

Table.1 showing avalanche effect of different techniques

ncryption Algorithm	File Size(KB)	%
Caesar cipher (26 bit)	50	2%
Vigenere cipher	50	4%
The Playfair cipher	50	8%
Rail Fence Technique	50	1%
DES	50	60%
Proposed Encryption (256 bit)	50	70%

CONCLUSION

Security and Privacy of data in Cloud computing is an area which has full of challenges. Cryptographic techniques are used for secure communication between the user and the cloud. Symmetric encryption has the speed and computational efficiency to handle large volumes of data in cloud storage. Some classical symmetric encryptions are described in this paper and evaluate with proposed technique. In this paper proposed a symmetric encryption algorithm for secure data of cloud user in cloud storage. The proposed algorithm is described in details. This algorithm is used in order to encrypt the data of the user in the cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication for the user. By applying this encryption algorithm, user ensures that the data is stored only in secured storage space and it cannot be accessed by administrators or intruders. So this algorithm increases the trust of user for storing data in cloud storage. The proposed technique used in future for powerful security on data that are stored in cloud.

REFERENCES

I. Christos Kalloniatis, Haralambos Mouratidis, Manousakis Vassilis, Shareeful Islam, Stefanos Gritzalis, Evangelia Kavakli, Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts, Computer Standards & Interfaces 36 (2014) 759–775.

II. Dawei Suna, Guiran Changb, Lina Suna and Xingwei Wanga, Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments,

Elsevier, Procedia Engineering 15 (2011) 2852 – 2856

III. Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A., Security and privacy in cloud computing: A survey, In Semantics knowledge and grid (SKG), 2010 sixth international conference on 1–3 November 2010 (pp. 105–112). Beijing, China: IEEE.

IV. Mackay M, Baker T, Al-Yasiri A, Security-oriented cloud computing platform for critical infrastructures, Elsevier, computer law & security review 28(2012)679e686.

V. Hassan Rasheed, Data and infrastructure security auditing in cloud computing environments, Elsevier International Journal of Information Management 34 (2014) 364–368.

VI. Avinash Kak , Classical Encryption Techniques Lecture Notes on Computer and Network Security, Purdue University, 2015.

VII. William Stallings, Cryptography and Network Security: Principles& Practices, Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2010.

VIII. Juraj Somorovsky, Mario Heiderich, Meiko Jensen, Jörg Schwenk, All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces, Copyright 2011 ACM 978-1-4503-1004-8/11/10.

IX. http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher.

X. http://www.math.tamu.edu/~dallen/hollywood/breaking/v.htm.

XI. http://en.wikipedia.org/wiki/Rail_fence_cipher.

XII. Fauzan Saeed, Mustafa Rashid, Integrating Classical Encryption with Modern Technique, IJCSNS International Journal of Computer 280 Science and Network Security, VOL.10 No.5, May 2010.

XIII. Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, Mohiy Mohamed Hadhoud, Evaluating, The Performance of Symmetric Encryption Algorithms, International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010.

XIV. Siani Pearson, Privacy, Security and Trust in Cloud Computing, HP Laboratories, HPL-2012-80R1, appeared as a book chapter by Springer, pp 1-56, 2012.

XV. Quist-Aphetsi Kester, A Hybrid Cryptosystem Based on Vigenere Cipher and Columnar Transposition Cipher, International

Journal of Advanced Technology & Engineering Research (IJATER), Volume 3, Issue 1, pp 141-147, 2013.

XVI. Singh Simon, the Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, ISBN 0-385-49532-3, 2000.

XVII. Frank Gens et al, Cloud Computing, An IDC Update http://www.cionet.com/Data/files/groups/Cloud%20Computing%202010%20-%20An%20IDC%20Update.pdf , 2010.

XVIII. Hashizume K. et al., "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013