Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data-Security

M. Raghuvaran Reddy,
Department of CSE,
Chickballapur,
India.

***Abstract*--- Cloud computing is a large pool of easily and accessible virtualized resources, such as hardware, development platforms and services. The main problem associated with cloud computing is data privacy, security etc. In this paper proposed the new level of data security solution with encryption using ASCII full characters. The main scope of this paper to solve the security issues in both cloud providers and cloud consumers.**

Keywords*--- *Cloud computing, Security, Encryption algorithms, ASCII code

1. INTRODUCTION

Cloud computing is a broad solution that delivers IT as a service. Cloud is an internet based technology uses the internet & central remote servers to support data and applications. It permits consumers and businesses putting to use without installation and approach their personal files at any computer with internet access. Before cloud computing, websites and server based applications were executed on a specific system [3]. The cloud computing flexibility is a function of the allocation of resources on authority's request. And the cloud computing provides the act of uniting.

A cloud is a pattern of parallel and distributed system be composed of a collection of interconnected and virtualized computers that are dynamically stipulation and presented as one or more unite computing resources established on service level agreements found amongst negotiation between
the service supplier and consumer.

The concept of cloud computing is linked closely with those of Information as a service (IaaS), Platform as a service (PaaS), Software as service
(SaaS) all of which means a service-oriented architecture
[4].
There are four types of cloud computing models listed by NIST (2009): private cloud, public cloud, hybrid cloud and community cloud [1].

1. Public Cloud: The cloud computing resource is shared exterior, someone can use it and a few payments maybe count. Public organizations assist in supplying the infrastructure to carry out the public cloud.

2. Private Cloud: private cloud resource is boundary to a collection of people, like a staff of a company. Infrastructure of private cloud is perfectly controlled and corporate data are completely supported by the organization itself.

3. Hybrid Cloud: This is the combination of public as well as private cloud. It can also be explained as multiple cloud systems that are related in a way that permits programs and data to be moved comfortably from one system to another.

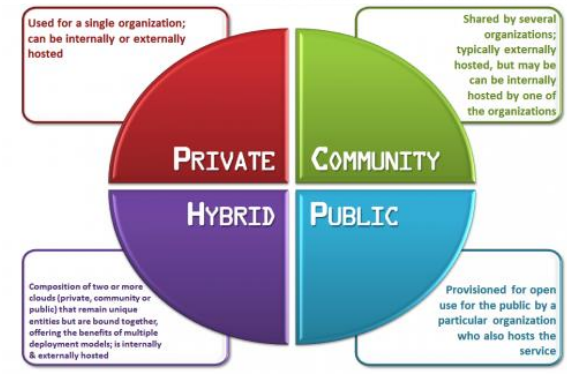
4.Community Cloud: The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause (mostly security).Infrastructure is to be shared by several organizations within specific community with common security, compliance objectives. It is managed by third party or managed internally. Its cost is lesser then public cloud but more than private cloud.

5.Distributed cloud: Cloud computing can also be provided by a distributed set of machines that are running at different locations, while still connected to a single network or hub service. Examples of this include distributed computing platforms such as BOINC and Folding@Home. An interesting attempt in such direction is Cloud@Home, aiming at implementing cloud computing provisioning model on top of voluntarily shared resources

6.Inter cloud: The Intercloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based. The focus is on direct interoperability between public cloud service providers, more so than between providers and consumers (as is the case for hybrid- and multi-cloud)

7.Multi cloud: Multicloud is the use of multiple cloud computing services in a single heterogeneous architecture to reduce reliance on single vendors, increase flexibility through choice, mitigate against disasters, etc. It differs from hybrid cloud in that it refers to multiple cloud services, rather than multiple deployment modes (public, private, legacy).

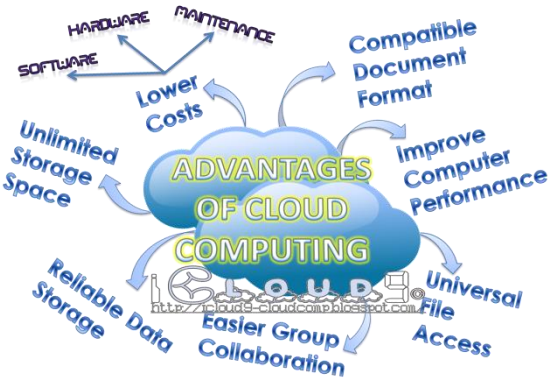
Figure. 1 Types of Cloud Computing



Advantages of Cloud Computing [2]

a) Reduced cost: Cloud technology is paid incrementally, saving organizations money.
b) Increased Storage
c) Organizations can store more data than on private computer systems
d) Highly Automated
e) No longer do IT personnel need to worry about keeping software up to date?
f) Flexibility
g) Cloud computing offers much more flexibility than past computing methods
h) More Mobility
i) Employees can access information wherever they are, rather than having to remain at their desks

Figure. 2: Advantages of Cloud Computing



II. SECURITY CHALLENGES IN CLOUD COMPUTING

The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, There by infecting the entire cloud.

There are five types of issues [6] raise while discussing security of a cloud;

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues
5. Trust Issues

1. Data Issues:

Whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data.

Data stealing [16] and Data loss is a common problem in cloud computing data issues.

2. Privacy Issues:

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect[8] the customer's personal information.

3. Infected Application:

Any malicious user [10] from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

4. Security issues:

Cloud computing security must be done on two levels. One is on provider level and another is on user level. The user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action [15].

5. Trust Issues:

Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider. So the vendor uses this marvelous application should make trust. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services.

III. EXISTING METHODS FOR DATA SECURITY IN CLOUD

Encryption is a well known technology for protecting sensitive data. Use the combination of Public and Private Key encryption to hide the sensitive data of users, and cipher text retrieval. The following three papers analyze the feasibility of the applying encryption algorithm for data security and privacy in cloud storage.

Neha Jain and Gurpreet Kaur [13] described Data security system implemented into cloud computing using DES

algorithm. This Cipher Block Chaining system is to be secure for clients and server. The security architecture of the system is designed by using DES cipher block chaining, which eliminates the fraud that occurs today with stolen data. The algorithm steps are follows.

1. Get the Plaintext.
2. Get the Password.
3. Convert the Characters into binary form.
4. Derive the Leaders (L1 to L16) from the Password.
5. Apply the Formula to get the encrypted and decrypted message.

The main contribution of this paper is the new view of data security solution with encryption, which is the important and can be used as reference for designing the complete security solution.

- Parsi Kalpana, Sudha Singaraju [14] have proposed a method by implementing RSA algorithm to ensure the security of data in cloud computing. RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. The purpose of securing data, unauthorized access does not allow. RSA consists of Public-Key and Private-Key. In the proposed Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

- Maha TEBAA et al [12] have proposed an application of a method to execute operations on encryp ted data without decrypting them which will provide the same results after calculations as if the authors have worked directly on the raw data. The author work is based on the application of fully Homomorphic encryption to the Cloud Computing security considering: Analyze and the improvement of the existing cryptosystems to allow servers to perform various operations requested by the client. The improvement of the complexity of the Homomorphic encryption algorithms and compare the response time of the requests to the length of the public key.

Comparison [17] among the above three existing methods precedes the insecure issues. So we are using the effective authentication plan to provide stronger security for both cloud providers and consumers.

IV.PROPOSED WORK PLAN

One of the simplest examples of a substitution cipher is the Caesar cipher [9]. It is said to have been used b y Julius Caesar to communicate with his army. Caesar is considered to be one of the first persons to have ever employed encryp tion for the sake of securing messages. Caesar decided that shifting each letter three places down the alphabet in the message would be his standard algorithm, and so he informed all of his generals of his decision, and was then able to send them secured messages. One of the strengths of the Caesar cipher is its ease of use and this ease of use would be important for Caesar since his soldiers were likely uneducated and not capable of using a complicated coding system.

Further enhancement to original three places shifting of character in Caesar cipher uses modulo twenty six arithmetic [5] encryption key that is greater than twenty six.

$$En(x) = (x+n) \bmod 26$$

The most pressing weakness of this cipher is simplicity of its encryption and decryption algorithms; the system can be deciphered without knowing the encryp tion key. It is easily broken b y reversing encryption process with simple shift of alphabet ordering [11].

$$Dn(x) = (x-n) \bmod 26$$

The earliest ceaser cipher method include the main drawbacks is plaintext and key is used only 26 alphabets. This paper overcome the above problem to plaintext is used case sensitive, numbers and special characters in order of ASCII full characters (256 char). This proposed method providing the inverse of Caesar cipher that supports more security for the data compared with the earliest Caesar cipher. And also it can be used simply encode the message for preserving privacy. It is complicated to understand the cipher text compared with the other methods.

Algorithm Procedure

Step1: Get the plaintext from the user (Ei) E-Encrypted text, I Text length.

Step2: Get the key value from the range numbers (0 to 256) (Ki) K-Key value, i Key length.

Step 3: Apply the formula Ei (X+K) Mod 256 or Ei (X+K) –256.

Step 4: Decryption Ei (X-K) Mod 256 or Ei (X-K) – 256.

Example

Consider the following example,

Plain text = Ascii; key value = 10;

ASCII value is 65, the fixed key length is 10, so encrypt the value using addition, but the ASCII code include 256 characters, let subtract the value with ASCII code.

Finally the value of the corresponding symbol is encrypted text.

- s ASCII value is 115, the fixed key length is 10, so encrypt the value using addition, but the ASCII code include 256 characters, let subtract the value with ASCII code.

Finally the value of the corresponding symbol is encrypted text.

- c ASCII value is 99, the fixed key length is 10, so encrypt the value using addition, but the ASCII code include 256 characters, let subtract the value with ASCII code.

Finally the value of the corresponding symbol is encrypted text.

- i ASCII value is 105, the fixed key length is 10, so encrypt the value using addition, but the ASCII code include 256 characters, let subtract the value with ASCII code.

Finally the value of the corresponding symbol is encrypted text.

- i ASCII value is 106 (***The repeated characters encryption using the character string = plaintext char + 1, so i+1(105+1) =106.consider decryption i-***

  1(105-1) =104), the fixed key length is 10, so encrypt

  the value using addition, but the ASCII code include

  256 characters, let subtract the value with ASCII code.

Finally the value of the corresponding symbol is encrypted text. A ASCII value = 65 (+)
Key = 10
75 (-)
ASCII TABLE 256

181

s ASCII value = 115 (+)
Key = 10
125 (-)
ASCII TABLE 256

131

c ASCII value = 99 (+)
Key = 10
109 (-)

ASCII TABLE 256

147

i ASCII value = 105 (+)
Key = 10
115 (-)
ASCII TABLE 256

141

i ASCII value = 106 (+)
Key = 10
116 (-)
ASCII TABLE 256

140

Plain text = Ascii
Key value = 10
Cipher text = T=1a^0^1’1^

V.CONCLUSION

Cloud computing is a new condition that isfamiliarizing in business surroundings where users can communicate directly with the virtualized resources and safe the cost for the consumers. Data security has become the most important issue for cloud computing security. Though many solutions have been proposed, many of them only consider 26 alphabets only. The main scope of this paper is the new level of data security solution with encryption using the ASCII full characters, which is important for designing the complete security solution.

REFERENCES

[1] Booth.D,(2004).web service architecture.Retrived from http://www.w3.org:http//
[2] Cong wang ,Qian wang, and Kui ren ,Wenjing lou,”Ensuring data storage security in cloud computing” at IEEE(8-1-4244-3876-1/09)
[3] Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.cm.
[4] Cloud computing methodology, systems and applications lizhe wang, rajiv Ranjan.http://www.unitiv.com.
[5] Dulaney E.,CompTIA Security+ Study Guide, Fourth Edition, Wiley Publishing Inc., Indiana,2009

[6] F.A.Alvi, B.S.Choudary, N.Jaferry,"Review on cloud computing security issues & challenges", iaesjournal.com, vol (2) (2012).
[7] John Harauz , Lori M.Kaufman ,Bruce potter,"Data security in world of cloud computing" by IEEE computer and reliability societies,jul/Aug 2009 pp 61-64.
[8] Jagpal Singh,Krishnan lal and Dr.Anil kumar Shrotiya, Journal of Computer Science and Applications., ISSN 2231- 1270 Volume 4, Number 1 (2012), pp. 1-7. http://www.irphouse.com
[9] http://en.wikipedia.org/wiki/caesar_cipher, Caesar cipher (Last accessed: April 20, 2012).
[10] Kevin Hamlen, Murat kantarcioglu, Latifur Khan and Bhavani Thurasingham, International Journal of Information Security and Privacy, 4(2), p.p(39-51), April-June 2010.
[11] Luciano D. and Prichett G., "Cryptography: from Caesar Ciphers to public-key Cryptosystem",The College Mathematics Journal,vol 18, no 1, pp. 2-17, 1987.
[12] Maha TEBAA, Saïd EL HAJJI and Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012 Vol 1 WCE 2012, July 4 - 6, 2012, London, U.K
[13] Neha Jain and Gurpreet Kaur, "Implementing DES Algorithm in Cloud for Data Security ", VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.
[14] Parsi Kalpana, Sudha Singaraju,"Data Security in Cloud Computing using RSA [15] http://www.mytestbox.com/miscellaneous/cloud-computinggrid- computing-utility- computing-list-top-providers/
[15] Security analysis of cloud computing: (http://cloudcomputing.sys-con.com/node/1330353).
[16] VAMSEE KRISHNA YARLAGADDA and SRIRAM RAMANUJAM "Data security in cloud computing ", vol.2 (1), pp. (15-23) (2011)
[17] Veerraju Gampala, Srilakshmi Inuganti and Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.