IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

A Review Paper on Enrichment of Data Security by using Various Cryptographic Algorithms

Varsha Gupta[1], Astha Gautam[2], Ruchi Singh[3]

M.Tech Scholar, Dept of Computer Science Engg, LRIET, Solan, Himachal Pradesh, India[1]

Assistant Professor, Dept of Computer Science Engg, LRIET, Solan, Himachal Pradesh, India[2, 3]

Abstract: Cloud computing has become trend in IT industry for storing, retrieving and maintaining the data over the internet. The advantage of cloud computing is easy accessing of data, reduced hardware, low maintenance and installation cost. But it is tough to preserve the data security and privacy. Thus the security has become the major issue in cloud computing because malicious user attacks the data easily by using various hacking techniques hence in this paper we discussed about various encryption algorithm and describe how encryption algorithms protects the data from intruder.

Keywords: Cloud computing, IT industry, encryption algorithms, data security and privacy.

I. INTRODUCTION

Cloud computing can be define as the process of storing, maintaining, retrieving the data remotely. It provides online storage of data, infrastructure and applications [1].

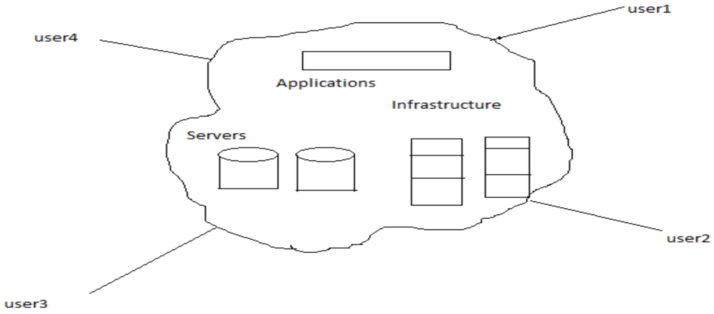

Fig. 1. Cloud Computing

(i) Application: Application is an online tool through which an user accessing the content .Google and facebook are the common examples of application.
(ii) Storage: Cloud computing offers to store the data over the internet rather than processor's hard drive .For e.g. Google drive, drop box, Gmail.
(iii)Infrastructure: Cloud infrastructure refers to hardware and software component. Servers, storage, a network and virtualization come under hardware and software that are needed to support the computing requirements of a cloud computing model.

Advantages
(i) Flexibility: In cloud computing resources can be increased or reduced depending upon workload.
(ii)Lower IT infrastructure cost: By using cloud computing we need not to invest in larger number of more powerful servers, we also need not to require IT staff for handling such powerful severs.
(iii)Mobility: Cloud computing provides mobility it means we can access our data from anywhere in any time.
(iv)Scalable: It quickly builds, deploy and manage applications, users and ability to build and expand with in time.

Disadvantages
(i)Require constant internet connection: Cloud computing is impossible without internet connection. If we want to access any data or document we need a constant internet connection.
(ii)Stored data might not be secure: Data is stored on remote servers so data is no longer in our hand. Hence data can be hacked by third party by applying various techniques [5].

DOI10.17148/IJARCCE.2017.6731

The idea behind cloud computing is that storing or sharing the data over the internet so that it would make easier to access the information however there are certain things that one must be aware of when using the cloud to store data. The serious thing in cloud computing is data security. If the data is not handled properly a hacker can be able to access confidential information because all information is shared through internet [2]. This can be prevented by taking certain security measures.

Deployment Models

Deployment model define the types to access the cloud. There are four types of deployment models.

Public cloud: It allows system and services to be easily accessible to public. Google is the example of public cloud. Cost effective, reliability, flexibility and location dependent are the benefits of public cloud [6]. Data is less secure in case of public cloud because data is managed by third party.

Private cloud: Private cloud allows system and services to be accessible within a single organization. Data is more secure in case of private cloud because data is handled within an organization. Only those user can access it who has authorization of accessing it[6].

Hybrid Cloud: It is mixture of private cloud and public cloud. Non critical activities are performed by public cloud and critical activities are performed by private cloud.

Community Cloud: Community cloud allows system and services to be attainable by a group of organization It shares the infrastructure from a specific community. Suppose two IT companies want to store their employee's data. Instead of making their own cloud they use the community cloud in which data of both the companies are processed.

Service Models

Cloud computing is based on service models these are SAAS, PAAS, IAAS.

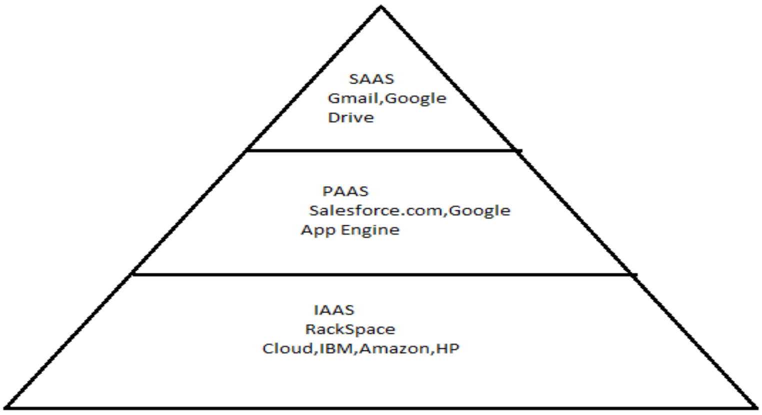

Fig. 2.Cloud Service Models

SAAS (Software as a service): SAAS is a method delivers web services over the internet. Application is accessed via internet. Gmail, Google drive are the common example of SAAS .In this service model user access application without worrying about security, managing application. User just needs to use the application. SAAS providers manage security, infrastructure and platform.

PAAS (Platform as a service): It provides platform to customers to develop, run and manage application without complexity of building and maintaining infrastructure. Google app engine, salesforce.com are the example of PAAS model.

IAAS (Infrastructure as a service): IAAS provides hardware, storage, server, and datacenter space and network components to the customer. In IAAS service customer has its own operating system and software. They need a administrator to configure the services, a software developer to deploy the application and to run the application [6]. Rack space cloud, IBM, HP, AMAZON are the example of IAAS service.

In Cloud computing data can be in various forms like images, files, text, audio and video. Because data resides on internet server so data can be hacked easily [5].To overcome this issue various encryption algorithm is implemented.

DOI10.17148/IJARCCE.2017.6731

An encryption algorithm along with a key is used in the encryption and decryption of data. Through the use of an algorithm, information is made in to meaningless information and requires the use of a key to transform the data back in to its original form.

There are two types of encryption:1) Symmetric Encryption 2)Asymmetric encryption.

In **symmetric** encryption same key is used for encryption and decryption. The sending party uses the secret key as a part of mathematical operation to encrypt plain text to cipher text [2].The receiving party uses the same key to decrypt the cipher text to plain text .Example of symmetric encryption algorithm is DES, 3DES, AES etc.

Plain text- Plain text is a message which is to be sending to receiver.

Cipher text- It is meaningless information which consists of plain text and a key.

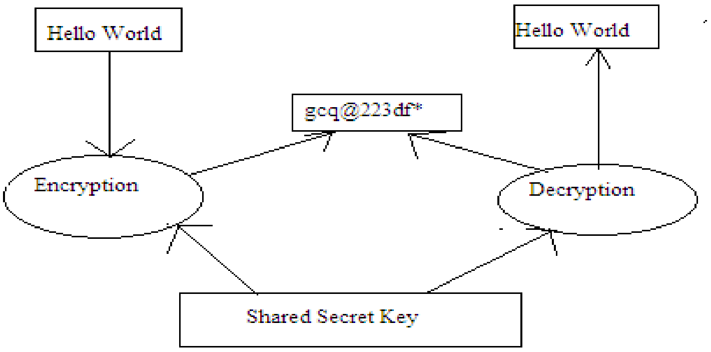

FIG .3. Symmetric Encryption Algorithm

In **asymmetric** encryption algorithm we use two keys for encryption and decryption i.e. private key and public key[2]. Public key is available to all including hackers .Private key is a secret key which is only known to the user .When sender wants to send data to the receiver he used receiver public key to send the message. He encrypts the plaintext with public key and cipher text is obtained .When receiver wants to read the data he decrypt that message by using his private key and cipher text .Example of asymmetric encryption algorithm is RSA.

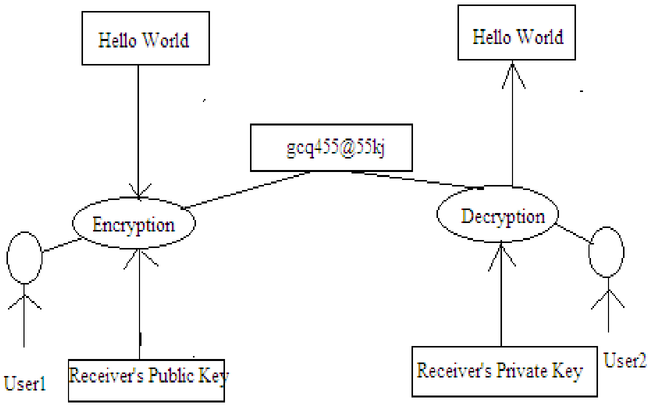

FIG .4. Asymmetric encryption Algorithm

II. LITERATURE REVIEW

B.kezia .et al [6] discussed about cloud computing and its types, various service models. They have also described the architecture of inter cloud, need of inter cloud and some of research challenges in inter cloud.

Madhumita Panda [9] proposed a framework in which comparison of encryption algorithm takes place on the basis of computing resources such as CPU time, memory and battery power. In this paper they took different types of files like binary file, text file and image file for comparison of encryption algorithms.

DOI10.17148/IJARCCE.2017.6731

Aamer Nadeem. et al [1] implemented four symmetric algorithm DES, 3DES, AES, and BLOWFISH out of them the best one was opt . In this paper performance of the algorithm compared by encrypting input file of varying contents and sizes on different hardware platform.

Vishwanath's mahalle[4] presents the paper in which hybrid (rsa+ aes)encryption is implemented to secure the data from intruder this hybrid approach involves 1) how to upload data securely by using a appropriate keys of rsa and aes 2) maintained integrity after downloading the data from the cloud .

Chang liang liang ning ye [10] proposed a hybrid encryption of rsa and aes to improve the security issues on light weight data like images, text and files. This paper first improve the rsa algorithm by increasing the length of rsa key so that it can quickly generate big prime and then merging the improved rsa and aes algorithm to secure the confidential data from the third party.

Nasreen khanezaei [3] presents a combination of rsa and aes encryption method to secure the cloud data the proposed method allows providing difficulty for attackers as well as reducing the time of information transmission between user and cloud data storage.

Vartika Kulshreshtha[8] paper describes about the performance of different security algorithm aes, rsa, and md5 for ensuring security framework. They compare these algorithms on the basis of encryption time, decryption time, and memory usage and speedup ratio.

III. CONCLUSION

Cloud computing aims to use system and services via internet so that it would be easy to access the information. As the data process and store on internet data may hack easily. To deal with such security issues we have discussed about various security algorithm like AES, RSA, DES ,3 DES, BLOWFISH .In this paper we discussed how hybridization of symmetric and asymmetric encryption algorithm RSA+BLOWFISH, RSA+AES leads to high security .In future we can enhance our data security by hybridizing symmetric encryption algorithms.

REFERENCES

[1] Aamer Nadeem, Dr M Younus javed, 'A performance comparison on data encryption algorithm' IEEE 2005.

[2] M Vijay priya, 'Security algorithms in cloud computing: overview', International journal of computer science and engineering technology, 2012.

[3] Nasrin khanezaei Zurina Mohammad hanapi, 'A Framework based on RSA and AES encryption algorithm for cloud computing services' ,2014 IEEE Conference on Systems, Process and control(ICSPC),12-14 December 2014 .

[4] Vishwanath S Mahalle, Aniket K shahade, 'enhancing the data security in cloud by implementing hybrid (RSA and AES) encryption algorithms', IEEE 2014.

[5] Farukh shezad, 'State of the art survey on cloud computing security challenges, approaches and solutions' ,The 6th International Symposium on Applications of Ad hoc and Sensor Networks pp. 357-362,2014.

[6] B.kezia rani, Dr B.Padmaja rani, Dr A.vinaya babu,' Cloud computing and inter cloud-types, topologies and research issues', 2nd International Symposium on Big Data and Cloud Computing pp. 24-29, 2015.

[7] Rizwana sheikh, Dr M.sasi Kumar, 'Data classification for achieving security in cloud computing', International Conference on Advanced Computing Technologies and Application pp.493-498, 2015.

[8] Vartika Kulshreshtha, Dr Seema verma and Dr C.Rama and K. Challa, 'A Comprehensive Evaluation Of cryptographic Algorithm in Cloud Computing', IEEE 2015.

[9] Madhumita panda, 'Performance analysis of encryption algorithm for security', International Conference on Signal Processing, Power and Embedded system, 2016.

[10] Chengliang, Ning ye, Reza Malekian, Ruchuan Wang, 'The hybrid encryption algorithm of light weight data in cloud storage 2nd International Symposium on Agent, Multi-agent Systems and Robotics August 2016'.

DOI10.17148/IJARCCE.2017.6731