ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Secure Transmission of Data in Cloud Environment Using Elliptic Curve Cryptographic Algorithm

Sridevi.R [1], Rahinipriyadharshini.R [2]

Assistant Professor, Dept. of Computer Science, PSG College of Arts & Science, Coimbatore, Tamilnadu, India[1]

Research Scholar, Dept. of Computer Science, PSG College of Arts & Science, Coimbatore, Tamilnadu, India[2]

ABSTRACT: Information security is the process of securing the private information in communication channel. Securing of private data and infrastructures becomes more crucial than ever. With the incredible growth of sensitive information on cloud, cloud security is getting more important than even before. The cloud data and services can be accessed anywhere. With the rapid growth of the cloud users disastrously happen with a growth in malicious activity in the cloud. Due to those malicious activities, every day, new security advisories are published in order to predict the more and more vulnerabilities which are discovered on the cloud. Billions and Millions of users are surfing over the Cloud for various purposes, therefore Security, privacy and authentication is highly needed for transmitting data over the cloud. This can be achieved by using the cryptographic algorithms to protect the private information over the cloud. Symmetric and Asymmetric are the two types of algorithms that are used in cryptography for encrypting and decrypting the text. The information which are used on the internet is highly confidential and not for public viewing. In this paper, we propose an Advanced Encryption Standard (AES) algorithm for data protection where data or sensitive information is encrypted before it is launched in the cloud, thus ensuring data confidentiality and security.

KEYWORDS: Information security, cryptography, AES algorithm, ECC algorithm, encryption, decryption, cloud.

I. INTRODUCTION

The term cloud computing means storing and accessing data and programs over the internet instead of your computer's hard drive. Cloud computing represents today's most exciting computing paradigm shift in information technology and it promises with several attractive benefits for businesses and end users. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel or licensing new software. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. Security and privacy are perceived as primary obstacles to its wide adoption. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. In this paper we have discussed about the data security in the cloud computing which can be achieved by using the cryptographic algorithms.

II. CRYPTOGRAPHY

Cryptography is the science of securing of data using mathematics or images which are to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks. So that it cannot be read by anyone except the intended recipient. The result of strong cryptography is cipher text that is very difficult to decipher without possession of the appropriate decoding tool. A cryptographic algorithm works in combination with a key, a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

A. *Cryptographic techniques:*
There are two types of cryptographic techniques were used for hiding the data.
i. Symmetric cryptography

- In symmetric cryptography same key is used for both encryption and decryption process. The key must be kept secret, and is shared by the message sender and recipient**.**

ii. Asymmetric cryptography.

- Whereas in asymmetric cryptography pair of keys called public and private keys used to encrypt and decrypt a message so that it arrives securely.

III. TYPES OF CLOUD COMPUTING

IT people discuss about the three different kinds of cloud computing where different services are being provided for you. The services such as IaaS, SaaS, PaaS has been discussed below.
A. *Infrastructure as a Service (IaaS) :*
Iaas is a kind of service which allows the user of cloud computing buying the access to raw computing hardware like storage or server over the net. It works on the principle of pay-as-you-go, based on the principle the cloud user can buy what he/she needs in cloud network. Ordinary web hosting is simple example for Iaas and of this kind of computing is often known as utility computing. By paying monthly subscription the hosting company will upload the file or services you're your website from the server which you need on the cloud computing to transmit the packet is considered as the network lifetime.

B. *Software as a service(Saas):*
Zoho is a kind of Saas provider which provides a variety of applications over the net. User of cloud networks uses the complete application of someone which is running on the someone's systems. Web based email and Google document are the best examples of Saas service.

C. *Platform as a service (Paas):*
Web based tools are used for developing applications so they run on systems software and hardware which is provided by another company. The best examples of Paas are Force.com and the Google App Engine.
The below given diagram represents the cloud computing with the above mentioned services such as Iaas, Saas, Paas. Which offers on demand self service, resource pooling, broad network access, rapid elasticity and measured Service for the cloud users.

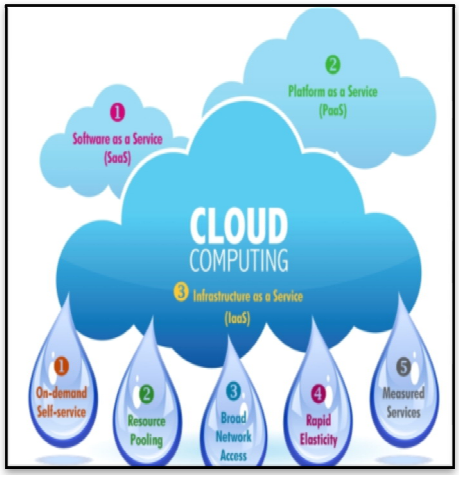

Fig: 1 Cloud Environment

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

IV. SECURITY AND PRIVACY CONSIDERATIONS IN CLOUD COMPUTING

This section describes the core considerations for any agency planning a deployment of a cloud computing service. Each area is described in some detail followed by a list of key considerations to assist agencies in developing an assessment of their risk position for a proposed service.

A. *Value, Criticality and Sensitivity of Information:*
Agencies are required to classify official information in accordance with the guidance published in 'Security in the Government Sector 2002 (SIGS)' 5. They are also required to protect official information in line with the guidance published in the 'New Zealand Information Security Manual (NZISM)' 6.

B. *Data Sovereignty :*
The laws that could be used to access information held by the service provider vary from country to country. In some instances when a service provider is compelled by a foreign law enforcement agency to provide data belonging to their customers, they may be legally prohibited from notifying the customer of the request.
Therefore it is critical that an agency identify the legal jurisdictions in which its data will be stored, processed or transmitted. Further, they should also understand how the laws of those countries could impact the confidentiality, integrity, availability and privacy of the information.

C. *Privacy Agencies:*
Planning to place personal information7 in a cloud service should perform a Privacy Impact Assessment (PIA) 8 to ensure that they identify any privacy risks associated with the use of the service together with the controls required to effectively manage them. Service providers typically use privacy policies to define how they will collect and use personal information about the users of a service.

D. *Confidentiality:*
There are many factors that may lead to unauthorized access to, information stored in a cloud service. However, it is important to note that the vast majority of these are not unique to cloud computing.

E. *Authentication and Access control:*
The adoption of multiple cloud services may place an unacceptable burden on users if the agency does not have an appropriate identity management strategy. The broad network access characteristic of cloud computing amplifies the need for agencies to have strong identity lifecycle management practices. This is because users can typically access the information held in a cloud service from any location, which could present a significant risk as employees. Permissions are approved at the appropriate level within the organization.

- Role Based Access Control is sufficiently granular to control permissions.
- Users are only granted the permissions they require to perform their duties.
- Users do not accumulate permissions when they change roles within the organization.
- User accounts are removed in a timely manner when employment is terminated.

F. *Encryption:*
The primary purpose of encryption is to protect the confidentiality of data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications. Encryption provides confidentiality, authentication, integrity, non repudiation.

G. *Data persistence:*
It can be difficult to permanently delete data from a multi-tenanted cloud service when the organization scales down or terminates its use of the service. If data is not securely deleted a future compromise of the service may still expose agency information. Similar issues arise if the service provider does not have processes to ensure that ICT equipment and storage media are securely wiped before disposal. Therefore it is essential that organizations to establish the service provider has robust and demonstrable data destruction and disposal processes in place.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

H. *Data integrity:*
Service providers can provide significantly different levels of protection against data loss or corruption. Some providers include data backup services as part of the base service offering, others offer them as an additional cost service and some do not offer them at all. Data loss or corruption could lead to information being permanently lost.

Fig 2: Applications of cloud

V. CRYPTOGRAPHIC ALGORITHMS FOR DATA SECURITY IN CLOUD COMPUTING

A. *Symmetric encryption algorithm:*
Is a technique to camouflage the originality of contents of blocks or streams with message file, encryption key and the password? Single key is used to encrypt or decrypt data. There are two kinds of symmetric-key encryption algorithms are used to wrap-up the content in a mask namely. Symmetric algorithms such as Block cipher, Ceaser cipher DES, AES, triple AES etc,

B. *Asymmetric encryption algorithm:*
Asymmetric cryptographic algorithm uses two different keys for encryption and decryption of the message. The public key is made publicly available and can be used to encrypt messages. The private key is kept secret and can be used to decrypt received messages. By keeping the private key safe, you can assure that the data remain safe. But the disadvantage of asymmetric algorithm is that they are computationally intensive.

VI. EXISTING ALGORITHM

Symmetric key cryptosystem has been used for encrypting and decrypting the data over the cloud. The data owners encrypt the each and every data before it is outsourced in the cloud network. Authenticated person has accessed the data with the help of the secrete key which has been sent by the data owner before data outsourced to user in cloud environment. AES algorithms were used in the existing system for encryption and decryption process. AES is a symmetric encryption algorithm used in cryptography which uses single key for both encryption and decryption process. The key is known as the secrete key which has been shared between the sender and receiver. Sender while sending the information to the receiver along with the information transfer the secrete key. The receiver can decrypt the data with the same key and transfer to the receiver. With the help of the secrete key again the decrypted text has been converted into plaintext which is the actual text in readable format. AES takes less time for encrypting and decrypting the text when compared other symmetric key algorithms. The main problem in the existing system is sharing of the secrete key and security. Once the secrete is missed between the two parties then it is difficult for both sender and receiver for sharing the data and this is the stage where both parties freeze in their communication.

VII. PROPOSED ALGORITHM

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. An elliptic curve over a field K is a non singular cubic curve in two variables, f(x,y) =0 with a rational point. The field K is usually taken to be the complex numbers, real, rational, and algebraic extensions of rational, p-adic numbers, or a finite field. Elliptic curve cryptography is a public-key cryptosystem.Where every user has two keys namely public and a private key. Public key is used for encryption/signature verification. Private Key is used for decryption/signature generation. This paper illustrates the proposed algorithm which has been used for the secure

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

transmission of data in the cloud network. The proposed algorithm Elliptic curve cryptography has been used to overcome the problems of the existing system.

eq. (3)

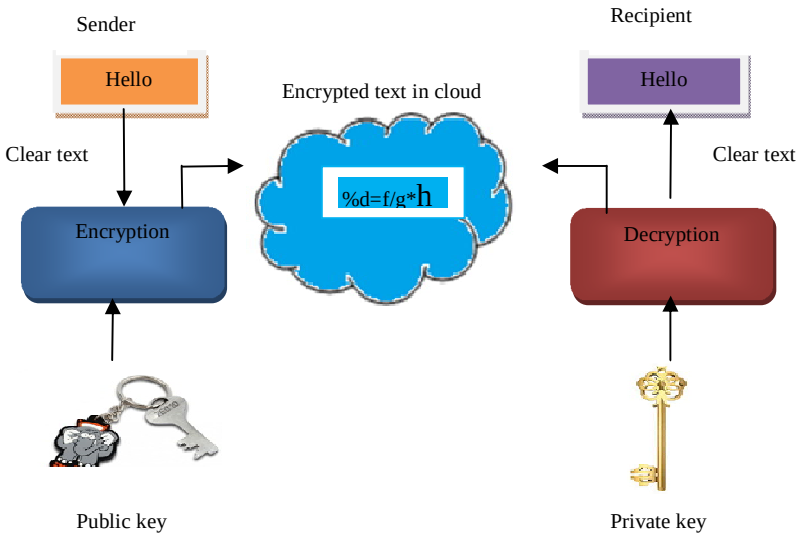

Fig3: Encryption and decryption using ECC algorithm

VIII. PROPOSED ALGORITHM USED FOR DATA SECURITY IN CLOUD NETWORK

Encryption algorithm
Private Key dA, Public key QA=dAP.

SIGNATURE GENERATION

Step 1: Select a random *k* from [1, *n*-1].
Step 2: Compute *kP*=(*x*1, *y1*) and *r=x1mod n.* if *r*=0 goto step 1
Step 3: Compute *e=H* (*m*), where *H* is a hash function, *m* is the message.
Step 4: Compute *s=k-1*(*e+dAr*) *mod n.* If *s*=0 go to step 1.
(*r, s*) is Alice's signature of message *m*

Decryption algorithm
Signature verification

Step 1: Verify that *r, s* are in the interval [1,*n*-1]
Step 2: Verify that *r, s* are in the interval [1,*n*-1]
Step 3: Compute *e=H*(*m*), where *H* is a hash function, *m* is the message.
Step 4: Compute *w=s-1 mod n*
Step 5: Compute *u1=ew mod n* and *u2=rw mod n.*
Step 6: Compute *X=u1P+u2QA*=(*x*1, *y1*)

Step 7: Compute *v=x1 mod n*
Step 8: Accept the signature if and only if

v=r

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Asymmetric Algorithms	ECC	AES
80	163	1024
112	233	2240
128	283	3072
192	409	7680
256	571	15360

Table1. Comparable Key Size (in bits**)**

Key Length		Time (s)	
AES	ECC	AES	ECC
1024	163	0.16	0.08
2240	233	7.47	0.18
3072	283	9.80	0.27
7680	409	133.90	0.64
15360	571	679.06	1.44

Table 2: Key generation performance of AES and ECC

The above presented table shows the key size of the AES and ECC. Whereas in ECC algorithm provides the strong security even if the given key is less when compared to the AES algorithm. And also presented the performance of both the algorithms based on the result produced by the given key length. When the key length 163 is given ECC encrypt and decrypt the text or data in 0.08 seconds and is more after then AES.

VII. CONCLUSION

With the tremendous usage of cloud computing the users of the cloud computing facing more security problems while transferring their data over the cloud network. The privacy of users at risk results from last control of data. Users of the cloud computing most concerned about their data security, confidentiality, reliability and more authenticated. This paper describes how the security can be achieved by using of elliptic curve cryptography algorithm in cloud computing. This paper provides the security to the data between the cloud networks. The above said authentication, security, confidentiality, reliability can be easily achieved by implementing the elliptic curve cryptography in the cloud computing.

VII. FUTURE ENHANCEMENT

Due to the rapid increase in the growth of network connectivity, the issue of network security is becoming increasingly demanding as far as size and implementation of new information technologies is concerned. Security is not a new issue and now it is recognized as one of the most complex problems like confidentiality, integrity, authentication, authorization. Proposed algorithm is designed to solve those problems. When compared to other cryptographic algorithm Elliptic curve cryptography provides solution for secured cloud environment with improved and high performance in computing power as well as battery usage and can been implement in the applications of cloud computing. The proposed work will be useful for cloud vendors and also for small and large investors of cloud computing.

REFERENCES

1. Vanya Diwan et al., “Cloud Security Solutions: Comparison among Various Cryptographic Algorithms” International journal of advanced research in computer science and software engineering (IJARCSSE), April 2014.
2. Hashizume et al.,”An analysis of security issues for cloud computing”, Journal of Internet Services and Applications (jisa), April2013.
3. Rashmi, “A Survey of Cryptographic Algorithms for Cloud Computing”, International Journal of Emerging Technologies in Computational and Applied Science (IJETCAS), May 2013.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

4. Abhishek Mohta et al, Ravi Kant Sahu and LK Awasthi, "Robust Data Security for Cloud while using Third Party Auditor" in International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE),Volume No. 2, Issue 2,Feb 2012.
5. Dripto Chatterjee, et al "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" in International Conference on Communication Systems and Network Technologies (CSNT), June 2011.
6. Douglas Selent, "Advanced encryption standard" Rivier academic journal, volume 6, number 2, 2010.
7. Maulik P. Chaudhari and Sanjay R. Patel, "A Survey on Cryptography Algorithms", International Journal of Advanced Research in computer science and management studies (IJARCSMS),March2014.
8. Vishwa gupta et al., " Advance cryptography algorithm for improving data security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.
9. AL.Jeeva et al., "Comparative Analysis of Performance Efficiency and Security Measures Of Some Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Volume. 2, Issue 3, May-Jun 2012.
10. Mandeep Kaur et al., "Implementing Various Encryption Algorithms To Enhance The Data Security Of Cloud In Cloud Computing" VSRD International Journal of Computer Science & Information Technology, Volume. 2, 10 October 2012.