International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

SECURE CLOUD ENVIRONMENT USING RSA ALGORITHM

P.suresh
Research Scholar,
Department of computer science,H.H The Rajahs college (Autonomous)India

---***---

Abstract : *During the last decide, information security has become a major issue. encryption and decryption data have recently been widely investigated and developed because there is a demand for stronger encryption and decryption which is very hard crack. cryptography plays major roles to fulfillment these demands. now days, many of researcher have proposed many of encryption and decryption algorithm such as AES, DES, RSA, and others. an RSA system generally belongs to the category of pkcs . rsa encryption is one of the public-key method that have been popular, the rsa algorithm is used in many application. although the security of rsa is beyond doubt, the evolution in computing power has caused a growth in the necessary key length. the performance characteristics of rsa are observed by implement the algorithm for computation. in this paper, RSA was implemented through an asymmetric key algorithm ,encryption and decryption procedure over different key size.*

KEY TERMS

RSA algorithm, Cloud computing, Cryptography, Encryption and Decryption, symmetric and asymmetric algorithm.

1.INTRODUCTION

Cloud computing is biggest buzz in the computer world these days. Cloud computing is everywhere. the locality of physical resource and device being accessed are in general not known to the end user. it also provide service for users to build up, deploy and manage their applications 'on the cloud ',which involves virtualization of resources that maintains and manages by itself. NIST definition of cloud computing. cloud computing is a model for enabling convenient, on demand network access to a shard pool of configurable computing resources (eg, networks, server, storage, application ,and services)that can be rapidly provisioned and released with minimal management effort or service provider interaction". one of the first cloud offerings was cloud storage and it remains a popular answer. cloud storage allows data stored remotely to be temporarily cached on mobile phones, desktop computer, or other internet linked devices. security and cost are the top issues in this field and very greatly. five characteristics-on demand self-service, board network access, resource poring, rapid elasticity, and measured service. four deployment model-private clouds, public clouds, community clouds, and hybrid clouds. three service model-software as service(saas),platform as a service(paas),and infrastructure as a service(iaas). it is important to highlights cloud computing is research challenges from an enterprise perspective because cloud computing is not simply about a technological improvement of data center but a fundamental change in how it is provisioned and used. companies such as Amazon , Google and Microsoft have invested waste sums money in building their public clouds and they seem to be leading the way in the technological innovation of cloud by rleasing frequent updates and new feature for there services. this paper cryptography technical using cloud computing. this cryptography can help emergent acceptance of cloud computing by more security companies. the first level of security where cryptography can help cloud computing is secure storge. cryptography is the art or science of keeping message secure by converting the data into non readable forms. now a days cryptography is considered as a combination of three algorithm .these algorithm as symmetric key algorithm, asymmetric key algorithm ,and hashing.this paper problem asymmetric key algorithm are those algorithm that use different keys for encryption and decryption.the two keys are private keys and public keys.public keys used by the sender for decryption and the private key is used for decryption of data by reciewer.in cloud computing asymmetric key algorithm used to generate keys for encryption.the most common asymmetric key algorithm for cloud are using rsa,ike,diffie helman key exchange.using asymmetric key algorithm based rsa cryptosystem realize the properties of the multiplicative homomorphic encryption.Ronald Rivist,Adi shamir and leonard Adleman hava invented the rsa algorithm and after is inventors.rsa uses modular exponential for encryption and decryption. RSA uses two exponents, a and b ,where a is public and b is private. so this paper of RSA , the primary advantages of RSA is increased security as the private keys do not ever need to be transmitted or revealed to anyone. where as in a secret -key system. there is always a change that an enemy could discover the security key while it is being transmitted. Another major advantage of publickeysystem is that can provide a method for digital signatures. Authentication via secret key system. a disadvantage of using public key cryptography for encryption is speed they are very slow in processing.

2.LITERATURE SURVEY

Rahul bhatnagar et al.(2013) in security in cloud computing have proposed an analysis of technical component and some research in threats for cloud computing users and threats for cloud service providers then provide many security, data and privacy protection, virtualization security, security arichitecture, model and frame work, security management and audit technology. shivashankar ragi(2011) with in a research thesis security approach for protecting data in cloud computing have described the security threats and identify the safety approaches for security in cloud computing and measured the protection challenges and security methods of clouds. in cryptography the advanced encryption standard(AES) is a symmertic key encryption standard. each of these cipher has 128-bit block size ,bit respectively[1]. survey of cryptography algorithm for cloud computing rashmi,manaoj jhuria,dr.shailendra.author discuss about the cloud computing is the emerging field in the modern era.cloud computing is defind as the set of resources or services offered through the internet to the user on their demand by cloud providers. it conveys everything as service over the internet based on user demand ,for instance operating system, hardware, srorag. resources, and software.cloud computing conveys everything as a service over the web supports user demand.to secure the cloud storage[2]. AES in cryptography the advanced encryption standard is a symmetric key encryption standard each of these cipher has a 128-bit block size, with size of 128,192 and 256 bit respectively. elliptic cureve cryptography provides confidentiality and authentication of data between cloud.it explores data security in cloud computing by implementing digital signature and encryption[4].during the data transformation to the cloud we use standard encryption method to secure the operation and the storage of the data. holomorphic encryption to execute operation and the storage of the storage of the data without decryption. it enables providing result of the calculations on encrypted data without knowing the raw data on which the calculation was carried out[5].the management of security in cloud computing ramgovind s.et.al[2010].in this paper author discuss about the management of the cloud computing. cloud computing is new and emerging information technology that changes the way it architectural solution are put forward by means of moving towards the theme of virtualization of data storage,of local networks as well as software cloud computing. has elevated it to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply. using cloud computing can help in keeping on as it budget to a bare minimum. cloud computing can computing can deliver a real time using many different types resources such as hardware, software, virtual storage once logged on to a cloud[6]. data security in cloud architecture based on diffie hellman and elliptical curve cryptography neha tirthani ganesan r. in this paper, author discuss about the data security in cloud computing. now a days, cloud computing becomes a difficult task. cloud computing refer to a network computer,connected through internet, sharing the resources given by cloud providers. cloud computing is a model for enabling convenient , on demand network access to a shared pool of configurable computing resources. the security in cloud computing is big issue the security threats such as maintenance of data integrity, data hiding and data safety dominate[7].

3.PROPOSED WORK

RSA: This is an internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, adi shamer,and leonard adleman.the RSA algorithm is the most commonly used encryption.till now it is the only algorithm used for private and public key generation and encryption.it is a fast encryption.

KEY GENRATION Before the data is encryption key generation should be done. this process is done between the cloud service provider and the user.

RSA ALGOPRITHM

1)SELECT two large prime number a and b.

2)compute n=a*b the computed n is made public.

3)now compute f(n)=(a-1)*(b-1).

4)choose a random number 'e' as the public in the range

1<e<f(n) such that GCD(e,f(n)=1.

5)find private key d such that $d = e^{-1}$ mod f(n), where d and f(n) are mutually prime.

ENCRYPTION

1)consider the user a that needs to send a message to b in secured manner using rsa algorithm.

2)now e is b's public key. since e is public, a is allowed access to e.

3)for encryption the message m of a whitch is in the range 0<M<N< IS converted to cipher.

4)where the cipher text $c = M^{e}\ mod\ n$

DECRYPTION

1)now the cipher text c is sent to b and a.

2)user b calculate the message with its private key β,where

ENCRYPTION

Consider the user a that needs to send a message to b in secured manner using rsa algorithm. now e is b's public key. since e is public, a is allowed accessed to e. for encryption the message m of a which is in the range o<m<n is converted to cipher. where the cipher text $c = M^{e}\ mod\ n$

DECRYPTION

Now the cipher text c is a sent to b from a.user b is calculated the message with its private key β, where message$M = c^{b}\ mon\ n$ RSA this an internet encryption and authentication system that uses an algorithm, based asymmetric encryption algorithm uses two keys instead of one. one is a private only known to the recipient of the message and the other is a public key known to everyone and can be freely distributed. either key can be used to encrypt and decrypt the message. however if only key a is used to encrypt the message then only key b can be used decrypt it.converse,it key b is used to encrypt the message then only key a can be used to decrypt it. RSA is the most common asymmetric cryptography algorithm. the minimum recommended key length is 1024 bits.

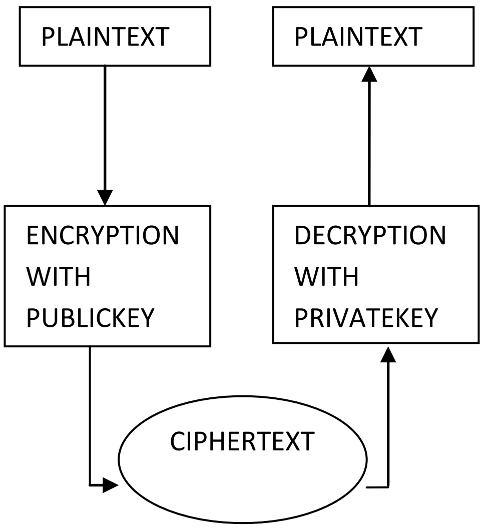


FIGURE 1:RSA ASYMMETRIC KEY

4.METHODOLOGY USED

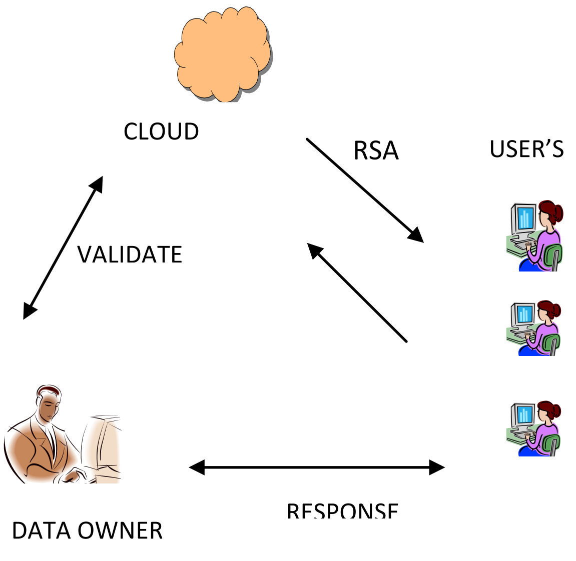


FIGURE 2: ARCHITECTUREOF RSA ENCRYPTION

RSA is widely used public key algorithm rsa stands for Ron Rives, Adi shamir and lenadleman ,who first publicly described it in 1977.IN OUR PROPOSED WORK, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it .by securing data, we are not allowing unauthorized access to it. user data is encrypted first and then it is stored in the cloud. when required, user place a request for the cloud provider, cloud provider authentication the user and delivers the data. RSA is a block cipher ,in which every message is mapped to an integer.RSA consists of public-key and private key. in our cloud environment, public key. it can be decrypted with the corresponding private-key only. SECURITY OF RSA , rsa consist of public key and private , public-key. for encryption and private key for decryption. key generation, encryption and decryption this soul of RSA algorithm. the security of rsa algorithm is lies on integer factorization problem. so the key selection is very impotent in rsa generally used said select a strongest key pair a and b to generate modules n. the condition of selection of a and b is both numbers. strong prime numbers have certain property. it's provide difficulty to factor n by using any specific factoring method (n=a*b), public key or encryption key (e,n) is known to ever one, if can factor n it's easy to discover d. so the selection of prime numbers is very important. otherwise the method used for selecting prime number must be efficient. this is the main feature of rsa. the key size decides the strength of cryptosystem. the size of rsa key typically refer to the size of n. if and b has larger size number with same length, it's very hard to factor the product n. the size of the key is depends on the security need. if the larger size it's provide good security on algorithm. this is cryptography algorithm which is used for encryption of plaintext to cipher vice versa. it uses mathematical computation for generating public and private key which are used for encryption or decryption purpose.rsa is used when secure data transmitted over the internet. in rsa cryptosystem, user share their public key with receiver for decrypting message. it keep secret it's private key. private key never shares with other users. rsa algorithm uses mathematical function to compute public or private key. it takes two large prime numbers and multiplies and applies some additional operation on it and generates. two set of keys. in rsa algorithm factor which is product after multiplying of two prime numbers. if any knows about the factor which is used in encryption process then the encryption can easily break.RSA encryption is strong when the factor are not disclosed, anyone can break the encryption.

5.EXPERIMENTAL RESULT

Secure the cloud manage data for cloud provider(csp).security goals of data include three points namely: confidential, integrity, and auditablity(CIA). confidentiality of data in the cloud is accomplished by encryption/decryption process. encryption/ decryption process in modern days is considered combination of two type of algorithm .they are (i)symmetric key algorithm cryptography such as data encryption standard (DES) advanced encryption standard (AES),Ronls code(RCN),and triple des. Asymmetric -key algorithm such as Rivest , shamir, and adleman(RSA),elliptic curve(EC),Diffi-Hillman(DH). In This Paper

FACTORS	DES	AES	RSA
CONTRIBUTER	IBM 75	RIJMAN JOAN	RIVEST SHAMIR 78
KEY LENGTH	56-BITS	128,192 AND 256	BASED ON NO.OF BIT IN N=A*B
BLOCK SIZE	64 BITS	128 BITS	VARTANT
SECURITY RATE	NOT ENOUGH	MEDIUM	GOOD

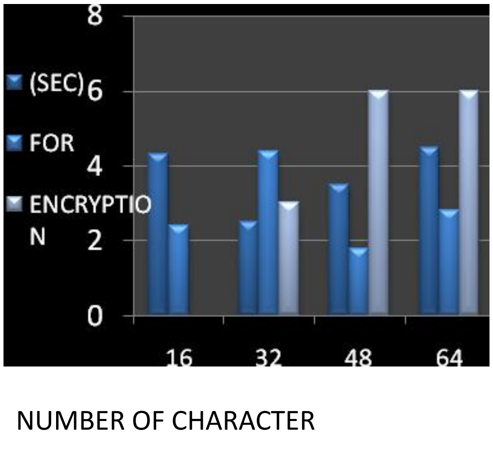
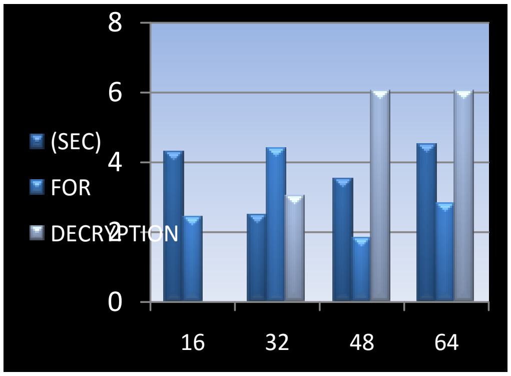


FIGURE 4: PERFORMANCE OF ENCRYPTION GRAPH

asymmetric algorithm are those algorithm which, use the same key for both encryption and decryption. hence the key is kept secret. symmetric algorithm have the advantage of consuming too much of computing power and it works with high speed in encryption. symmetric key algorithm are divided into two types: block cipher and stream cipher. in block cipher input is taken as a block of plaintext of fixed size is applied on to block of the same size as the block of plaintext is obtained. in rsa cryptosystem, used share their public key with receiver for decryption message. it keep secret it is private key never shard with other user. for this paper different type algorithm to compare secure algorithm.



NUMBER OF CHARACTER

FIGURE 5:PERFORMANCE OF DECRYPTION GRAPH

in this Table efficient cryptosystem can produce best possible result if key size comparable to the size packet to be transmitted over the network. algorithm on the basis of parameter like key length, block size, type and features.
As we know that the data is stored on some else location in the cloud computing so we need high processing speed as well as high security. here the graph shows the performance of our proposed scenario. Bars are showing that how much time it will take to encrypt data. different experimental result are shown in the graph which are done on the basis of different experiments.

6.CONCLUSION

cloud computing is the latest trend in it. but security is the biggest challenge in this area. each and every day new security prevention method is discovered, but it's not a permanent solution. encryption is the best security method , now different kinds of encryption technique apply in cloud computing environment , some extend hacking can be prevented in this way. so it's very important to provide a good level security in this environment is the one of decide the strength of the cryptosystem, when we selected large key size prime number, its cannot be easily factored and discovered. so provide a good level security the keys used should be powerful. but generation main problem of RSA is increasing key generation time when we select large key size number, the key generation time is also increase, this problem can be solved by applying asymmetric key algorithm. a drawback of RSA using public key cryptography for encryption is speed they are medium process. FUTURE scope using various algorithm as described cloud security can be ensured in real time environment.

REFERENCES

[1] Guannan hu and wemhao zhu "A dynamic user integrated cloud computing architecture" proceedings of the 2011 international conference on innovative computing and cloud computing(Iccc,11).pp3640,2011

[2] Rashmi nigoti,Manoj jura,D.r shalendra singh, A survey of cryptographic algorithm for cloud computing, international association of scientific innovation and research.

[3] Priyanka arora,aran singh,himanshu tyagi "Evaluation and comparison of security issues on cloud computing environment" in world of computer science and information technology journal.(WCSIT)ISSN:2221-0741 VOL.2,NO 5-179-183,2012.

[4] M.Sudha,Dr,Bandaru rama krishna rao,m.monica, a compare sensive approach to ensure secure data communication in cloud environment, international journal of computer application (0975-8887)volume 12-no 8,dec 2010,pp-19-23)

[5] Sameera abualrahaman almulla,chan yeobyeun, cloud computing security management engineering system management and is application(ICESMA),2010.

[6] Ramgovind s, eloff mm,smith e,the management of security in cloud computing, 978-4244.2010 IEEE.

[7] Neha tirthani ganesan r, data security in cloud architecture based on diffie hellman and elliptical curve cryptography.

[8] Birend ragoswami, dr.s.nsingh, enhance security in cloud computing using public key cryptography with matrices,(IJERA).vol:2 issue 4,pp(331-334)2012.

[9] Sheruf el-etrby, eman m.mohamed. modern encryption techniques for cloud computing, proceeding of the informatics and system 8th international conference ,cc-1,cc-6 year.2012.

[10] Saffer jaboudl , mohamed a.al- fayoumil,2-mustafa al-fayoowni 3rd haidar s.jabbar.an efficient rsa public key encryption. schema,15th international conference on

information technology new generation (page127-130)year 2008.