PERFORMANCE ANALYSIS ON HYBRID ALGORITHM IN CCSS MODEL THROUGH 3KDES, RSA, ECC ALGORITHM

Ritika Dubey[1], Apoorv Dubey[2], Vaibhav Doshi[3]
[1,2,3]Assistant Professor, Department of CSE, Jaipur (Rajasthan)

Abstract: As we seen that, today's generation of IT has widely use the cloud computing services, that means in future cloud computing will important part of IT enterprise. Today, if we are think to establish the new IT industry. We require the lot of hardware device or software, and some other infrastructure for all kind of think; we need money to purchase the software license, different hardware device and also need dedicated staff members to maintain. In fact, IT industry actually need complete the applications for that they require to work hard and to achieve certain efficiencies. Hardware and software equipment's are only enterprise with the tools. Hence, there are not any such services, which provide the software desired to service users, but only user only require to use the software again when demand billing it. In this model of service, user only require paying an amountof rent to the service provider or supplier, you can get the proper services, based on the mainconcept, our main concept is the secure data (in database) on cloud platforms for that we use some encryption techniques to secure the data in database and we also use the hybrid techniques, load balancing techniques. Effective result can be seen in backend of application.

Keywords: cloud computing, Encryption, RSA algorithm, DES algorithms, ECC algorithms, hybrid-encryption-algorithm, Database, CCSS Model (cloud computing security service model)

I. INTRODUCTION

Security is one of the most difficult task toimplement in cloud computing. The paper basically deals withthe security issues that are experienced during the storage ofdata on the cloud. The cloud vendors generally store theclient's data and information in cloud without following anysecurity measures.

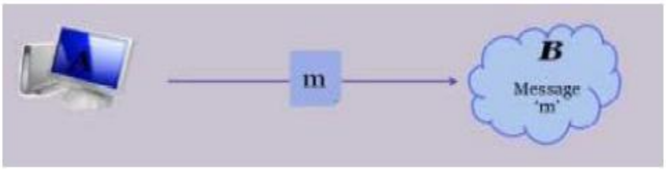


Fig.1. Data Uploaded in Cloud

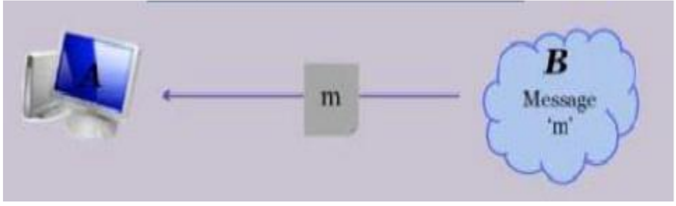


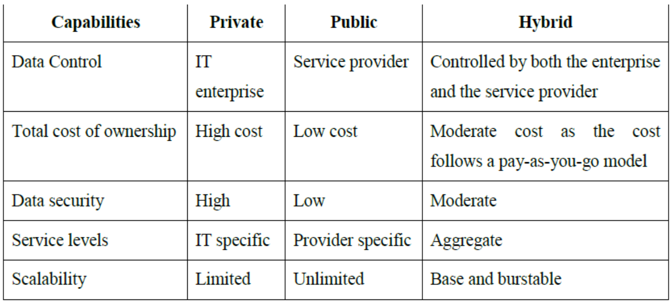
Fig.2. Data Downloaded from Cloud

Almost every cloud provider does not provideenough security measures to ensure the data safety and that'swhy clients waver keeping their data at some place which isvery easy to be accessed by someone else. For the security issues of cloud computing, the paper secures transmission ofdata storage and data security for both aspects into line research. Cloud data securitydesign into mass storage data storage and backup design methods and mechanismsdesigned to isolation. Guarantee the security of data stored in the cloud. To solve thesecurity of data transmission, this dissertation presents an improved hybridencryption algorithm 3kDES, in order to achieve the purpose of the data transmissionprocess secure encryption, and the improved algorithm and RSA, ECC algorithmsinto line performance testing and comparative analysis. While adding the datatransfers interrupt processing strategy to ensure the transmission of data security.

II. CHALLENGES IN THE CLOUD COMPUTING

- Quality of service guarantees
- Dependence on secure hyper visors
- Attraction to hackers
- Safety of virtual OSs in the cloud
- Possibility for substantial outages
- Encryption require for cloud computing
- Encrypting access to the cloud source control interface
- Encrypting administrative access to operating system instances
- Encrypting access to application and Encrypting application data at rest
- Data ownership issues
- Multi-tenancy

With the development of cloud computing, and enterprise users have different for different cloud computing knowledge and understanding. Some companies and personally think that all services and applications are available through the cloud platform to achieve, but the other part of the people think that, after all, the cloud platform calculated by cloud service providers to maintain and manage, the less important the core system and confidential data within the enterprise should own deployment and storage. Our security in the cloud, there are many studies. Malicious attacks on network one of theresults is the latest research an idea about cloud security strategy: When the network detectsthe presence of the latest viruses Trojans & other malicious program, put the news is sent tothe server for analysis and processing, and then send the results to each client, so that thenumber of users under such a huge case, so long as one client emergence of new Trojans andother malicious programs when you can immediately from service side to get a solution, thenthe solution can immediately get all the other clients.



Capabilities	Private	Public	Hybrid
Data Control	IT enterprise	Service provider	Controlled by both the enterprise and the service provider
Total cost of ownership	High cost	Low cost	Moderate cost as the cost follows a pay-as-you-go model
Data security	High	Low	Moderate
Service levels	IT specific	Provider specific	Aggregate
Scalability	Limited	Unlimited	Base and burstable

Table 1 Comparisons of the Three Types of "Cloud" Features.

III. RESEARCH ANALYSIS

Definitions[1] : Cloud computing is a computer class to provide the requested servicemodel of distributed resources, are generally based on virtualization technology anddistributed computing technology services idealized cloud computing system has a lot offeatures: highly abstract resources; Dynamic can scalability; readily available; many userscan share and use hardware and software resources, data resources; users on demand realtimeservices and service requests, pay-to; programmable management. At present, althoughthe definition of what has been widely recognized No, but identification of a computing model is not attributable to cloud computing mode.

Cloud computing allows users to calculate the service providers through a unified interface to cloud computing cloud platform provides access to on-demand power, storage capacity and a variety of application software services, resources on a cloud platform is dynamically allocated and managed, this unity The form is available through the internet service to the majority of users and enterprises, and the user does not know the overall structure and composition of the cloud [2]. Simple framework of cloud computing services shown in Figure 3.

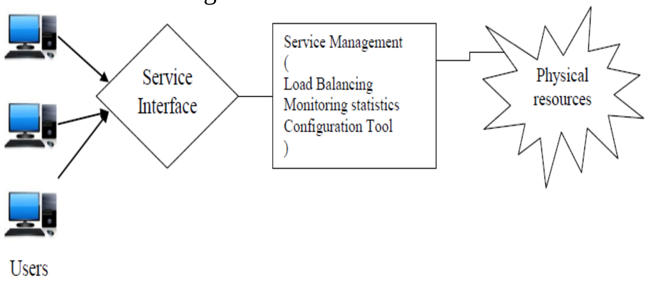
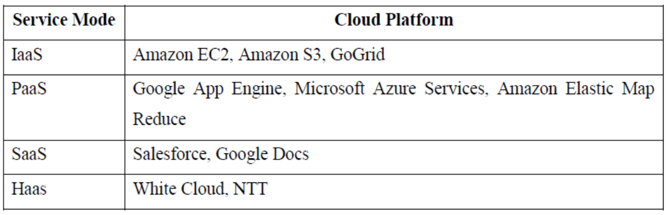


Fig. 3 The basic framework for cloud computing services

Initially, IaaS and HaaS are considered to be the foundation for consumer platforms provided by the network service provider using cloud computing facilities. After the order tomore clearly distinguish between these two, it will provide a special called virtualized IaaS infrastructure services. Both core users are providers of hardware, but the difference is that IaaS refers specifically to provide virtualized infrastructure services layer, The HaaSincludes all hardware facilities to provide infrastructure services layer. Currently the world's leading cloud platform Amazon EC2, Google Docs, etc., and they were used the corresponding service. Business model as shown in Table 2



Service Mode	Cloud Platform
IaaS	Amazon EC2, Amazon S3, GoGrid
PaaS	Google App Engine, Microsoft Azure Services, Amazon Elastic Map Reduce
SaaS	Salesforce, Google Docs
Haas	White Cloud, NTT

TABLE 2 Business Model

IV. RESEARCH METHODOLOGY

This paper gives a cloud-based service model, which is based on an existing cloudcomputing platform, security issues into the encrypted data storage and encryptiontechniques have two aspects one for design, and second for efficient[3]. The main problem isthe content of the resource load balancing algorithm cloud.

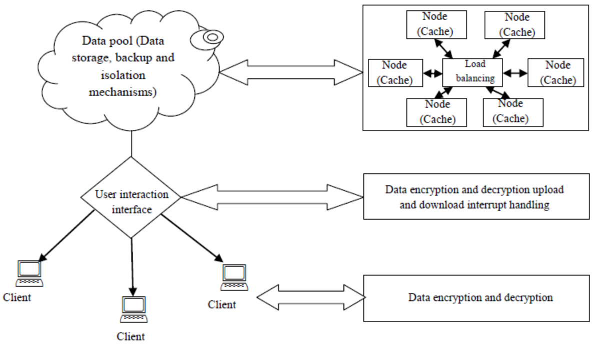

Data pool (Data storage, backup and isolation mechanisms)
Node (Cache)
Node (Cache)
Node (Cache)
Load balancing
Node (Cache)
Node (Cache)
Node (Cache)
User interaction interface
Data encryption and decryption upload and download interrupt handling
Client
Client
Client
Data encryption and decryption

Fig. 4 The overall structure of the service model based on cloud computing platform

From the application stage of thecloud computing platform provided the user application mainly via two steps: a first step register as a user of the application, the second step to manage their own data through clienttools, download it, and more or delete operation. This operation can be seen from twostorage systems need to do in two parts: First, save all users login information, and second,to save all the personal data of the user, which means that users can be divided into twomodes management and file storage blocks[4]. Process the entire massive data storage system shown in Figure 5.

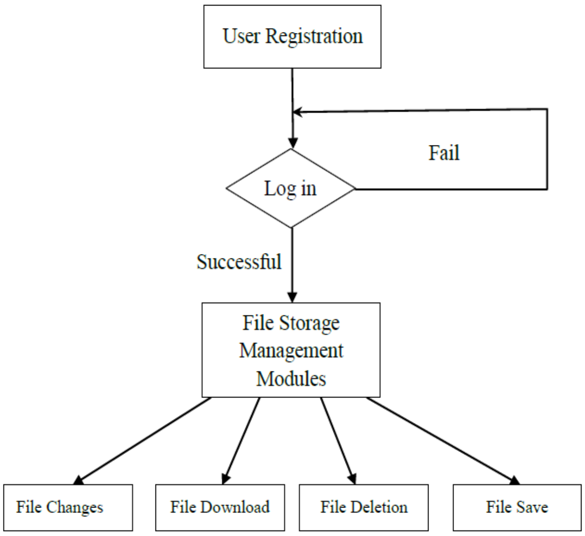


Fig. 5 Mass Data Storage System process

Copyright 2018.All rights reserved.

V. METHODOLOGY

DES algorithms

The algorithm works on the principle that the expressly in accordance with each group 64the size of the bit are grouped, and set the key length is 64 bits, and the key of the element is actually in a group 56-bit in DES operators, in clear text in the group data, combined withother 8-bit, but is actually a encryption of only 56-bit, and the other 8 bits are the parity bit.Through to the clear grouping of the initial displacement,16 the iterative transformation, andreverse-initial replacement and 16 sub key-generation process, and result is encrypted,Encrypted text and express the algorithm originating after entered is encrypted, and finallyfrom the output of the output[6].

The algorithm has three variables: key, data and mode. Thekey for encrypting and decrypting the key to use, data for the encryption and decryption ofdata, the mode of the algorithm for the model.The algorithm's simple process shown in Figure 6.

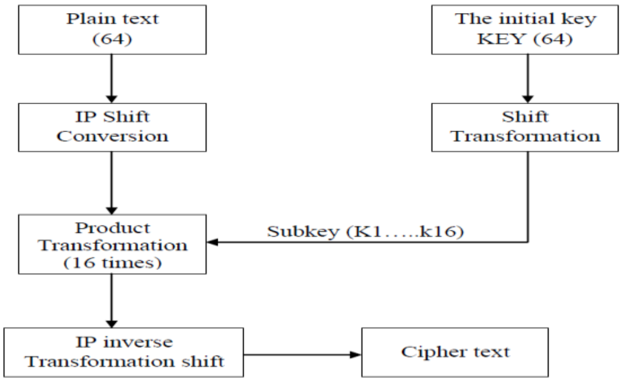


Fig. 6 DES Algorithm the simple process

DES algorithm's biggest advantage is encrypted at a faster rate, and as-on-a-chip technology continues to improve, more and more construction costs low, to improve DES-algorithm the computational speed for the effective technical support.

RSA Algorithm

In RSA cryptography techniques, both the public-key and the private-keys can encrypt a message or data; one use to encrypt a message and opposite key is used to decrypt massage. This attribute is one reason that why RSA has become the most popular algorithm and it's widely utilized. It gives a method of assuring integrity, authenticity, confidentiality, validity, data-storage and non-reputability of electronic communications[7].

RSA derives its security or safety from the difficulty of factoring large integer that is theproduct of two prime numbers. Multiplying these two numbers is very easy, but determiningthe same prime numbers from the total-factoring is measured infeasible due to the time itwould take even using today's super computers.

Disadvantages of RSA:

- Slow decryption, which is slightly difficult to implement securely.
- Very slow key-generation.
- Two-part key is helpless to GCD attack if weakly implemented.

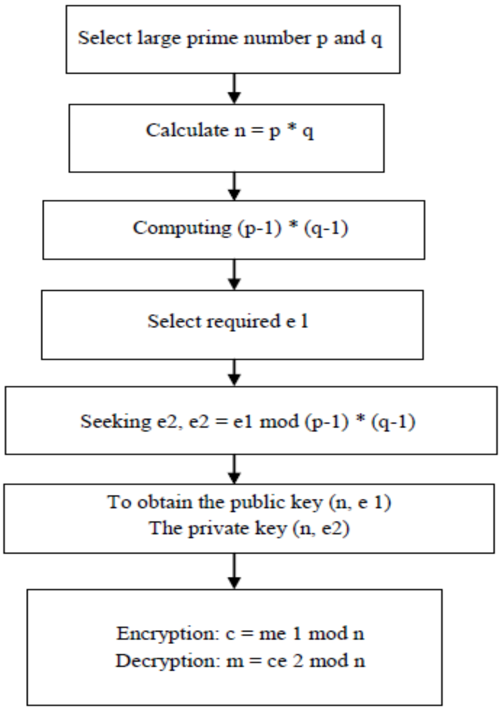
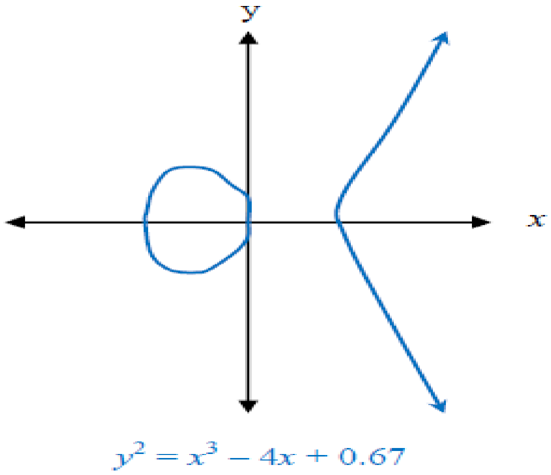

Select large prime number p and q
Calculate n = p * q
Computing (p-1) * (q-1)
Select required e 1
Seeking e2, e2 = e1 mod (p-1) * (q-1)
To obtain the public key (n, e 1)
The private key (n, e2)
Encryption: c = me 1 mod n
Decryption: m = ce 2 mod n

Fig. 7 The simple process of RSA algorithm

To use RSA keys to digitally sign a message, Alice would make a hash or message digest ofher message, encrypted the hash-value with her RSA private-key or secret-key and append itin to the message. Then send it to bob. Thenbob can decrypt the hash value with her publickey.If this value similar to the hash of the same message, then only Alice could have sent itthat characteristic know as authentication and non-repudiation and the message is exactly asshe wrote it. Alice could encrypt her message with bob's public-key before sending it.A digital certificate holds the information that identifies the owner and also holds theowner's public-key. Certificate is signed by the certificate authority that issues them, and canprocess of obtaining public-keys and authenticate the owner.

Elliptic Curve Cryptography (ECC) algorithm

A recent development in thisfield is known as ECC.ECC works with points on a curve. The safety of this type of publickeycryptography completely depends on the elliptic curve discrete logarithm problem.The main benefit of ECC is that keys can be much smaller. Recommended key's size is inthe order of 160bits rather than 1024bits for RSA[8]. ECC, An elliptic curve is a set of points (x, y), for which it is true that y2=x3+ax+b specifiedcertain selected numbers a and b. Normally the numbers are integers whole numbers, whilein principle the system also working with real fractional numbers. Despite what the namepropose, the curves does not have an elliptic figure such as a =-4 and b=0.67 provides theelliptic curve with equation y2=x3-4x +0.67. This curve is demonstrated in the following figure 8.



Encrypting and decrypting process: Bob and Alice can now secretly agree on a key withwhich they can encrypt messages by private-key. The key simply is the product of Alice'spublic-key and Bob's secret-key, which is the similar as the product of Alice's secret-key &Bob's public-key. It will be clear that Alice and Bob can compute this product after they

have share their public-keys, but Eve cannot since she has none of the secret-keys.

The elliptic-curve key cracking process: If Eve wanted to break the key, she would have torecreate one of the secret-keys. This means having to calculate AS given AP and F becauseAP=AS*F. And that is very hard. The number of discrete points on the curve is called thecurve's order. If the order of the point-F are a prime number of n bits, then calculatingAS from AS*F and F takes roughly 2n/2 operations.

Disadvantages of ECC

- Complicated and tricky to implement securely and safely, mainly the standardcurves.
- Signing with a broken random number generator compromises the key.
- Still have some patent problems, especially for binary-curves.
- Binary-curves are slightly scary.

Improvement of hybrid-encryption-algorithm

The discussions of DES-algorithm, RSA-algorithms and ECC-algorithm explain that any of the algorithms for individual use are often not able to fully meet cloud computing requirements of security and efficiency. This dissertation is the first three algorithm's advantages and disadvantages, and a based on DES algorithms and RSA, ECC algorithm to mix of encryption algorithm, which is symmetric-encryption algorithm and non-symmetric encryption algorithm. The improvements of the algorithms are characterized by confidentiality, safely, encryption is fast, and is not vulnerable to the attack, and so on; you can guarantee the security of as much as possible to maximize efficiency. Improvements process of the hybrid encryption algorithm shown in Figure 8.

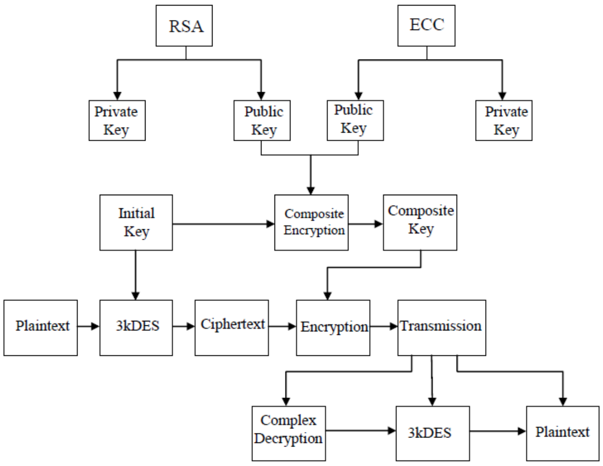
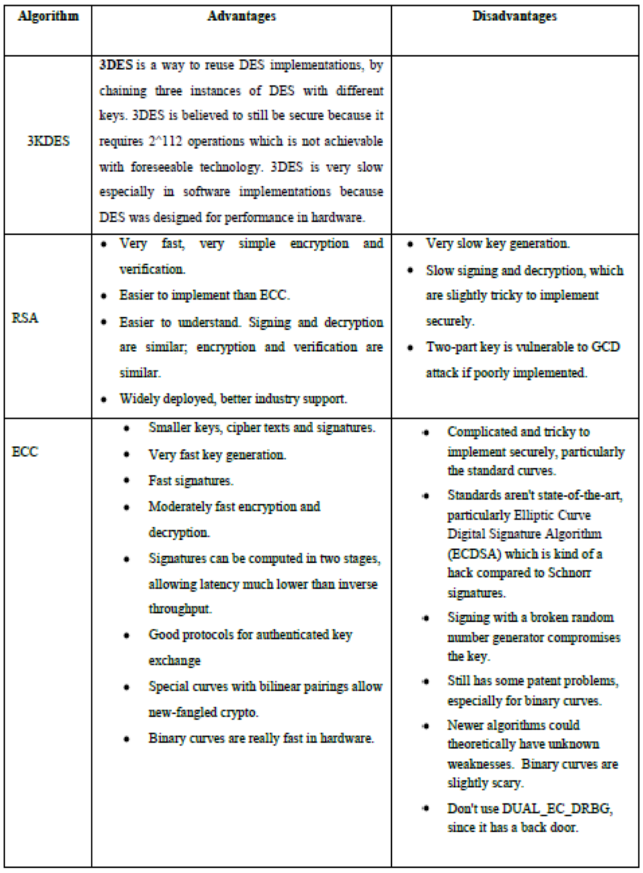


Fig. 8 Improvement of the hybrid Encryption Algorithm Processes

Due to DES encryption-algorithm has the benefits of fast speed and overcome thedisadvantages of short key length, this dissertation based on the DES-algorithm, designs akind of improved hybrid encryption algorithm 3kDES.3kDES algorithm is, for the datapacket or message three times DES encryption, this can increase key's length. Because thelength of key is too small to avoid the attack caused by, while it remain the same benefit andDES encryption algorithm faster maintained.



Algorithm	Advantages	Disadvantages
3KDES	3DES is a way to reuse DES implementations, by chaining three instances of DES with different keys. 3DES is believed to still be secure because it requires 2^112 operations which is not achievable with foreseeable technology. 3DES is very slow especially in software implementations because DES was designed for performance in hardware.	
RSA	• Very fast, very simple encryption and verification. • Easier to implement than ECC. • Easier to understand. Signing and decryption are similar; encryption and verification are similar. • Widely deployed, better industry support.	• Very slow key generation. • Slow signing and decryption, which are slightly tricky to implement securely. • Two-part key is vulnerable to GCD attack if poorly implemented.
ECC	• Smaller keys, cipher texts and signatures. • Very fast key generation. • Fast signatures. • Moderately fast encryption and decryption. • Signatures can be computed in two stages, allowing latency much lower than inverse throughput. • Good protocols for authenticated key exchange • Special curves with bilinear pairings allow new-fangled crypto. • Binary curves are really fast in hardware.	• Complicated and tricky to implement securely, particularly the standard curves. • Standards aren't state-of-the-art, particularly Elliptic Curve Digital Signature Algorithm (ECDSA) which is kind of a hack compared to Schnorr signatures. • Signing with a broken random number generator compromises the key. • Still has some patent problems, especially for binary curves. • Newer algorithms could theoretically have unknown weaknesses. Binary curves are slightly scary. • Don't use DUAL_EC_DRBG, since it has a back door.

Table 3:-Comparative chart

VI. ANALYSIS AND RESULT

To implement the hybrid encryption algorithm

Improvement method of 3kDES hybrid encryption algorithm described below:

(1) The encryption process

First, assume the plaintext space A, A's size according to each group 64, 64 is not thecomplement of the random 64, after the packet plaintext space as: A1A2A... Ai. Next, for allpacket encrypted according to 3kDES-algorithm, the cipher text set to B, the encryptionprocess is:

$Bi=kDESx_3(kDESx_2^{-1}(kDESx_1(Ai)))$

After we get the whole space-A plaintext encrypted as B1B2B3... Bi. An entire plaintext usesthe 3DES, a process for the encryption algorithm:

$B=kDESx_3(kDESx_2^{-1}(kDESx_1(A)))$

The next set of keys were used in the first step in encrypted X1, X2, X3is encrypted using theRSA algorithm and the ECC combined. First, the X1, X2, X3into Xr and Xs. Two parts,namely the use of ECC and RSA algorithms for the two parts of key groups encrypt:

Encryption using the RSA algorithm for Xr and generating cipher text Cr :-First set the RSA algorithm using large prime numbers has multiplied to n, the public key is

set to m, the RSA for Xr

Encryption process is:

$C_r=X_r^m$ mod n

Encryption using the ECC algorithm for Xs and generating ciphertext Cs:-First set of elliptic curve Ep (a, b), select a basis point on the curve G finite fields, supposingECC algorithm is key for k, choose a random number x, then the ECC for Xs

Encryption process is:

$Cs=Xs+X_{kG}$

Where: kG public key algorithm for the ECC.

As a result the encryption process is complete, we can send an cipher text using 3kDESalgorithm result as B, RSA encryption algorithm ciphertext Cr and ECC algorithm encryptedciphertext Cs,

The final form of the ciphertext isB + Cr+ Cs.

(2) Decryption process

When recipient receive the cipher text B + Cr+ Cs, we start the decryption process. Firstly,we set the RSA algorithm uses a large prime number multiplied n and private key is d,thedecryption process is

$X_r=(C_r)^d$modn

We get Xr with the help of RSA algorithm. Secondly, we set the ECC algorithm Csdecryptget Xs. it's the reverse process of ECC encrypted algorithm; the formula can be expressed as:

$X_s= C_s-X_{kG}$

Then we decrypt the ciphertext B, in fact, the reverse process of the encryption, is calculatedas:

$A = kDESx_1^{-1}(kDESx_2(kDESx_3^{-1}(B)))$

Thus the decryption process is completed, the finally obtained plaintext A.

Performance Analysis of cloud computing service model

Encryption algorithm to encrypt and decrypt, but at the same time will also consume some time encryption and decryption, also will consume part of the resources, the 3kDES algorithm and RSA, ECC algorithm to make a comparison and analysis of the performance, from and evaluate, the improved performance of this hybrid encryption algorithm.The main contents of the tests with threedifferent encryption algorithms to encrypt the data, thereby to obtain the time taken for theencryption, than the final comparative analysis based on test results.

Computation time	3kDES	RSA	ECC
1st test	43ms	456ms	421ms
2nd test	44ms	432ms	452ms
3rd test	46ms	467ms	483ms
4th test	47ms	487ms	473ms
5th test	49ms	492ms	437ms
Average time	45.8ms	466.8ms	453.2ms

Table 4 Shows The Three Encryption Algorithms Are Time-Consuming For A Small Amount of Data To Compare Data.

Table 4 shows that three data encryption algorithm is a small amount of time spent on themillisecond level, for the user, such as time magnitude will not bring significant impact onpeople. Next is the large amount of data obtained in the test case, Table 5 shows the threeencryption algorithms to encrypt the time spent large amounts of data comparison data.

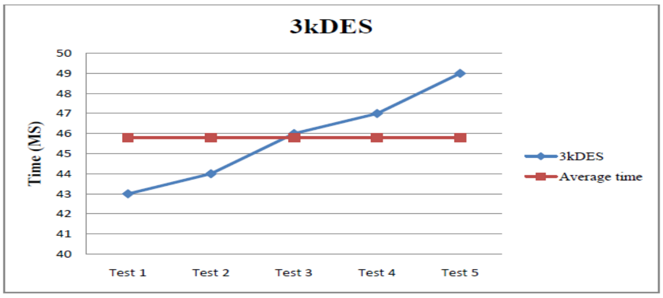


Fig. 9 3kDES in graph

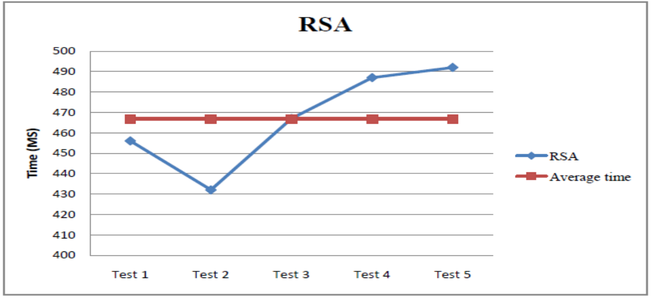


Fig. 10 RSA in graph

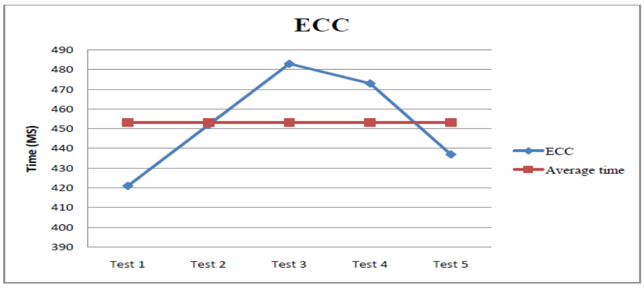


Fig. 11 ECC in graph

Computing time	3kDES	RSA	ECC
1st test	9.587s	198.322s	156.422s
2nd test	10.132s	178.457s	168.569s
3rd Test	9.876s	187.684s	178.436s
4th test	10.324s	197.486s	163.924s
5th test	10.432s	189.798s	154.639s
Average time	10.070s	190.349s	164.398s

Table 5 Three Encryption Algorithms To Encrypt A Large Amount Of Data The TimeSpent

The test results in Table 4 and Table 5 conclusion can also verifythis. So3kDES algorithm is suitable for large amounts of data to be encrypted. The RSA andECC algorithm in the processing of information due to its inherent operational mode leads toa lot of time consuming, is not conducive to the large amount of data to encrypt dataprocessing. Although RSA and ECC, they are not the speed of the algorithm encryptionalgorithm 3kDES.

Thus, 3kDESimproved algorithm for plaintext plus secret of time and the entire hybrid encryption algorithm to encrypt the plaintext time belong to the same order of magnitude above. Also,because 3kDES algorithm mechanism is based on symmetric encryption algorithm and itsadvantage is encrypted faster.

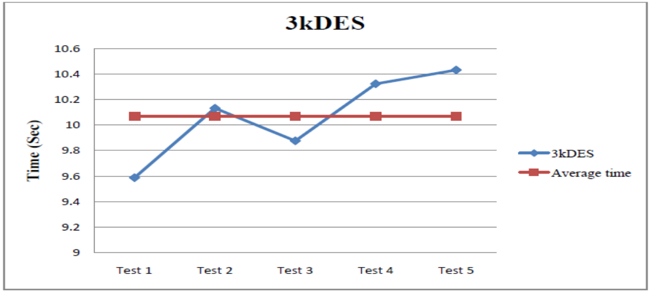


Fig. 12 3kDES in graph

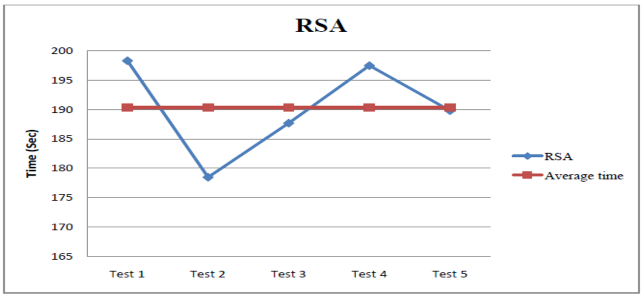


Fig.13 RSA in graph

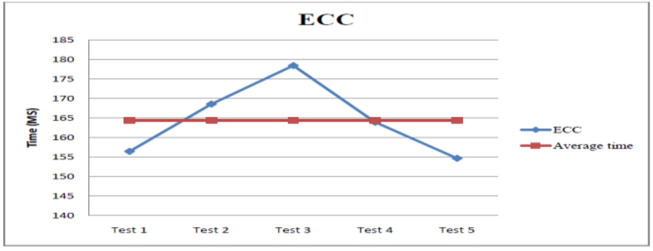


Fig. 14 ECC in graph

Finally, it can be concluded: improved 3kDES and RSA, ECC algorithm hybrid encryptionalgorithm in terms of efficiency and performance symmetric encryption algorithm isbasically the same, but in terms of security and public key encryption algorithm and fairly,this chapter presents the change into the hybrid encryption algorithm to ensure highersecurity while improving the efficiency of encryption and decryption, can well assure cloudoperator safety features of the service.

VII. CONCLUSION & FUTURE WORK

This research discusses the current cloud computing security problems and pitfalls faced in terms of efficiency, pointed out the cloud safety and efficiency aspects of the issue is an important reason to get the current constraints of cloud computing to promote and popularize the. For two heavy these issue, this dissertation proposes a service model based on cloud computing platform, designed to improve the safety and efficiency of cloud computing platform.

For the security issues of cloud computing, the dissertation secures transmission of data storage and data security for both aspects into line research. Cloud data security design into mass storage data storage and backup design methods and mechanisms designed to isolation. Guarantee the security of data stored in the cloud. To solve the security of data transmission, this dissertation presents an improved hybrid encryption algorithm 3kDES, in order to achieve the purpose of the data transmission process secure encryption, and the improved algorithm and RSA, ECC algorithms into line performance testing and comparative analysis. While adding the data transfers interrupt processing strategy to ensure the transmission of data security.

Cloud computing security and efficiency issues has been the core issue of concern, the focus of this study is also two problems this dissertation can also be further research work carried out in the following areas:

- Consider the optimization of load balancing algorithm between nodes by schedulingtasks between nodes so that resources are more reasonable allocation.
- Consider the need for the user to selectively encrypted data is encrypted, so that theservice model to become more intelligent.

I hope in the future to study and work, the work can be done for this study further optimization and improvement.

REFERENCES

[1] European Network and Information Security Agency Cloud Computing: Benefits, Risks and Recommendations for Information Security 2009-11-01. http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-riskassessment/at_download/fullReport. 2009.

[2] LM Vaquero, L Rodero-Merino, etal “A Break in the Clouds: Towards a CloudDefinition” ACM SIGCOMM Computer Communication Review, 39 PP: 50-55, 2009.

[3] W. Itani, A. Kayssi, A. Chehab “Privacy as a

Copyright 2018.All rights reserved.

Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures" IEEE International Conference onDependable, Autonomic and Secure Computing, pp 711-716, 2009.

[4] Fei Hu, Meikang Qiu, Jiayin Li, etal "Review on cloud computing: Design challenges in architecture and security" Journal of Computing and Information Technology, pp.25-55, 2011.

[5] Kaufman, "LM Data Security in the World of cloud computing" Security & Privacy,IEEE, pp: 61-64, 2009.

[6] Deng Qianni, Chen Quan "Cloud computing and its key technology Development andapplication of high performance computing", pp: 2-6, 2009.

[7] Jiang Xiaoqing, Yang Lei, He Binbin "future of new computing model", Cloudcomputing Computer and Mathematical Engineering, pp: 5-8, 2009.

[8] Sanjay Ghemawat "The Google File System", Proceedings of the 19th ACMSymposium on Operating Principles, pp: 20-43, 2003.

[9] Dean J, Ghemawat S. "Map Reduce: Simplified Data Processing on Large Cluster" The 6th Symposium on Operating System Design and Implementation SanFrancioso,CA, pp:149-167, 2004.

[10] Chen Shuping, Houxian Liang "Computer networks DES data encryption anddecryption technology" Modern electronic technology in, pp: 11-115, 2005.

[11] Eli Biham "How to decrypt or even substitute DES-encrypted messages in 228 steps".Information Processing Letters, 84 (3) pp:117-124, 2002.

[12] Juan C Asenjo "The Advanced Encryption Standard- Implementation and Transition toa New Cryptographic Benchmark". Network security, pp 7-9, 2000.

[13] Wang Qian, Ni Jianwei "based on RSA encryption algorithm" Chongqing University,pp. 68-72, 2005.

[14] Jasleen Kaur, Dr. Sushil Garg"Security in Cloud Computing using Hybrid ofAlgorithms", pp. 300-305, 2015.

[15] Galen Gruman. What is cloud computing? Http://www.infoage.idg.com.au/index.