IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 02 (February. 2014), ||V6|| PP 01-08

Improve Cloud Computing Security Using RSA Encryption WithFermat's Little Theorem

Balkees Mohamed Shereek*ZaitonMuda** SharifahYasin***
Faculty of computer science and information technologyUniversity Of putra Malaysia,43400 UPM serdang Selangor DarulEhsan, Malaysia

Abstract: - Cloud computing (CC) is new technology for hosting and delivering services over the Internet. It moves computing and data away from desktop and portable PCs into large data centers.CC is a Internet based computing, the entire data reside over a set of networked resources, this data can be accessed through virtual machines like i phone, PC etc.CC help to reduce hardware, maintenance and installation cost. But security and privacy is the two major issues in this field and it prevent users for trusting CC. Cloud computing share distributed resources in the open environment via the network, so it makes security problems .To keep user data highly confidentially against un-trusted servers and from malicious attacks is very important. Encryption is the one of the most secured way using prevent unauthorized access. Hence we provide a new method for Cloud Computing Security by applying RSA algorithm and Fermat's theorem together. Its help to build a new trusted cloud computing environment. By using Fermat's theorem can be speed up the RSA Encryption.

Keywords: *-Cloud computing, Decryption, Encryption, Fermat's little theorem, RSA*

I. INTRODUCTION

Cloud computing is a very broad term used for the recent development of internet.it is the new technology in the IT world, that share computer resources through internet instead of using software or storage on a local pc. The main advantage of cloud computing is cost saving. That means the customers do not have to pay for infrastructure and it's, installation.in cc its does not require to need the end user information, such as physical location and configuration of the system for provide the cc servieses.cloud computing has the concepts of parallel computing, distributed computing and grid computing [1].in cc, computing power, software, storage service and platforms are delivered to external user through internet. This resources and service can scale up and down to meet user requrments.the users need to charge the resource as pay-per use modal. This is the core concept behind cc. cloud computing is named as fifth generation of computing after main frame, personal computer, client-server and web[2].in cc the resources are available in distributed manner and clients can access the resource through internet using any kind of devises at anywhere of this world. Cloud computing also named as dynamic computing because its provide resource dynamically (as needed). A simple example of cloud services is a webmail. The technology of the cloud computing is service oriented architecture (SOA) [3].this architecture would make the cloud computing platform is more flexible, extensible and reusable. In cloud computing a set of rules called protocol and special software named as middleware are located at the central server administrator system. Its helps to monitoring cloud computing traffic and user demands [4].Security is playing a major role to the down acceptance of the cloud computing among the users. It's difficult to measure the quality of the cloud provider's security method because many providers will not ready to expose their infrastructure to the public [5].creating and managing a secure cloud space is challenging task.Cloud data security depends on applying appropriate data security Procedures and countermeasures. Each encryption methods have its own merits and demerits. So based on the problems mentioned above its need to an efficient and proper security schema in CC is very important.RSA is widely used Public-Key algorithm, generally it's consider more secure than other encryption algorithams.RSA security lies on the integer Factorization problem.Small encryption and decryption key were easily factored and discovered. To overcome this problem and provide a good level security the keys used should be powerful. The key size decides the strength of the cryptosystem. But the main draw backs of Rsa are compared with other encryption techniques is its take more time. Mainly time complexity process in RSA is key generation. This problem can be solved by applying Fermat's little theorem, by using this theorem during key generation process we can reduce the time. Once a data is encrypt by RSA algorithm, only the concerned user can decrypt this encrypted data.

This paper is organized as follows: section 2 discuss the basic concepts and challenges of cloud computing .Discuss about related work in section 3, it's followed by RSA algorithm in section 4. Existing RSA encryption techniques in cc is discussed in section 5,Discuss proposed method in section 6

II. CLOUD COMPUTING

Cloud computing is emerging paradigm, which mainly concentrate to provide dynamic, on-demand scalability of virtualized recourse to set of users. Scalability and virtualization is the two key factor of cloud environment. Because of the accessibility of the cloud computing services many researchers are focus to this area. According to forester he define cloud computing as "*A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption".*The main goal of cloud computing is achieve higher throughput by effective use of distributed resource [1].cloud computing provide different way to access and manage the cloud resourse.cc is an internet based computing.so users can be access the recourse through any kind of virtual machine .

Characteristics of cloud computing

1. Shared infrastructure:-sharing of physical services among the multiple users that means there is no resource are dedicated to one user it's pooled together to multiple consumers
2.On-demand self-service:-cloud is a large resource pool; user can buy the services according on their demands.
3. Virtualization:-in cloud computing can we access the data from anywhere through any kind of terminals.
4. Elasticity: - cloud computing have ability to allow the users to scale up their recourses at any time to addresses their heavy load and they can scale down if they need it.
5. Reliability:-

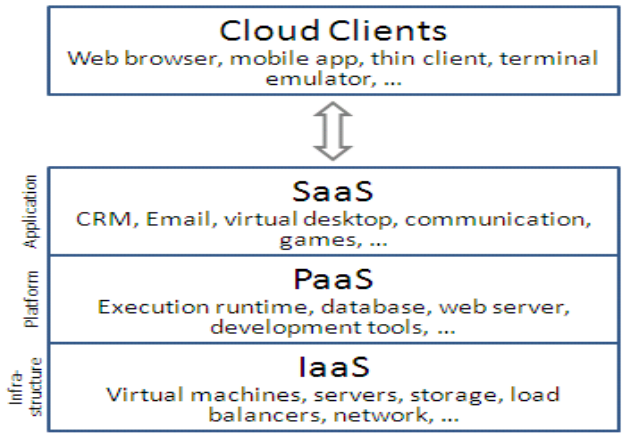
Clouds services can be grouped into three categorize.

1. Software as a service (SAAS) :-):- in this model the complete service are offered to the clients as their demands. It's a multi-tenet architecture i.e. A single instance of service can be access to many end users at a same time, and it's not affect the performance of the service. This model is avoided to buying and installing software at end user side. The key characteristics of saas is network based access and commercial availability of the software which are managed by the centralized location [4].Now the companies offered by saas service is google, Microsoft, zoho etc. benefits of saas models is

- Automatic update and patches management
- Global accessibility
- compatibility

2.Platform as a service(PAAS):-):-this is the middle layer, which offers platform oriented services.paas service contain a set of software and development tools which help to develop and run the clients application on their own local pc without having any idea about what's going on behind the services. This service provide a complete software development life cycle management, it's starting from planning and passed through design, building an application,deployment,tesing and finally its end with maintenance. Its help the cloud users to develop and run their own software on cloud platform without any formalities and cost. Google's App Engine, Force.com, etc. are some of the PaaS examples

Infrastructure as a service (Iaas):- it is the lowest layer that provides basic infrastructure services. Mainly it provides storage and computing capabilities. Main service of iaas is server, storage systems, networking equipment, data centre space etc. The main advantage is the customer pay only the time duration they use the services. Iaas helps the user to reduce the huge initial investment in computing hardware such as servers and network devices [5]. This is very similar to utility computing. Along with iaas and other services user can do their works without bothering anything about the underlying complexities. The cloud users do not manage the underlying infrastructure but they are controlled over OS, storage and deployed application etc. Examples of this model are amazon, GoGrid etc.



2.1 Types of cloud deployment model

Deployment model of the cloud computing are differ based on the requirements.

Public cloud**:-**cloud applications and storage are available to the general public by a service provider. It's run by third parties. Most of the public clouds are hosted away from the clients.comparitivily it's less secured than other models. All the applications and data's on the public cloud is highly chance to face the malicious attacks. This can be prevented by applying security methods on both sides. This service is free or pay-per usage modal. Main advantage of this modal is its reducing customer risk and cost.

Private cloud**:-**cloud applications and services are providing for a specific organization. The resources are not shared to others. Its consider more secure than other models and it is easier to mange.in private cloud all the resources and applications are managed by the organization itself.

Community cloud**:-**share the cloud applications between the several single organizations from a specific community based on the common concern.

Hybrid cloud**:-**combination of two or more private, public or community clouds. It's offering the benefits of multiple deployment model and each models are bond together. A gateway used to connect and manage the applications and data flow from each part to another.

Advantages of cloud computing

- Easy management
- Environmental friendly
- Scalability
- Cost reduction
- Availability

2.2 Cloud computing challenges

When a new technology is discovered it's also some another techniques is come with that, to destroy the new one. Cloud computing also faces this problem. The biggest concern about cloud computing are security and privacy [1] .protection and prevention is the one way to solve the isuues.the protection can be done by using proper authentication and authorization method this way we can solve the privacy issuess.Data loss, phishing and botnet is consider as well-known security issues and its cause to serious threats in cloud environment.multi-tenancy modal and resource pooling feature has introduce new security challenges[5] in cc have passive and active attacks[6].passive attacks is does not modify the data packets eg: release the content of the message. In active attacks, reading the message unauthorized way and modify the message. Threats and vulnerabilities this two factors are prevent the users to trust cc environment. Based on Cloud Security Alliance (CSA), Cloud vulnerabilities are core-technology vulnerabilities, essential cloud characteristic vulnerabilitiesetc. Basic security threats in cloud computing is failures in provider security, attacks by other customers, availability and reliability issues etc. [7].In cloud environment, its not have any border or limitation to store data, so data can be physically located anywhere in theworld [8].so this phenomena raise to series issue in cloud environment.Cloud data security distributed into three levels network level, host level and application level.identiti accessmanagement is help to mutualauthentication, authorization and auditing of cloud computing management [9].

III. RELATED WORK

Cloud computing technology suffers from threats and vulnerabilities, this prevent the users from trusting it. Occurrence of these threats may lead to damaging or illegal access of critical and confidential data of users. Illegal users have threatened this technology such as data misuse; inflexible access control and limited monitoring. In order to provide security in cloud against the various threats and attacks different cloud service providers adopt different techniques. Security of the transmitted data can be achieved through various encryption and decryption schemes [6] propose different encryption methods Identity Based Encryption, Linear Search Algorithm, Identity Based Signature etc. Elliptic Curve (EC) systems are applied in cloud environment for provide data security. Elliptic curve cryptography provides confidentiality and authentication of data between clouds. It explores data security in cloud computing by implementing digital signature and encryption. [10]. during the data transformation to the Cloud we use standard encryption methods to secure the operations and the storage of the data. Holomorphic encryption is a method to execute operations on encrypted data without decrypting .it enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out [11]. Another method is Propose [12] Public Key Cryptography with Matrices. It's have a three-stage secured algorithm. By using matrices application generate a system of non-homogenous linear equation and the security is based on solving this equation.[13] evaluate eight modern encryption techniques in two different platform one is Amazon cloud computing environment and another one is desktop eight modem encryption techniques is RC4,RC6, MARS, AES, DES, 3DES, Two-Fish, and Blow-fish and finally they find-out there is no strongindications in both enviornment.provide a vary user friendly

encryption method[14].users can select the various encryption algorithms as per their own choice propose four encryption algorithm, AES, DES, RSA and Blow-fish from this user can select one algorithm to ensure the Security of data in cloud.

IV. RSA ALGORITHM

In 1976, Diffe and Hellman find out a new type of cryptography called public key cryptography and it's have separate keys for encryption and decryption. The encryption keys known to public and its named as public key and decryption key is kept as secret key so it's called as private key .once a message is encrypted by the public key, it can be decoded only the person with have private key. Rivest, Shamir and Adelman published a first method of realizing public key cryptography in 1977.this method is called RSA. Security of RSA based on difficulty to factoring large numbers. RSA is widely used algorithm in many filed like e-commerce, bank, military etc. An exceptional good feature we can find out the RSA is component used in encryption is re-used during decryption process. i.e.

$C=M^e \mod n$

$M=C^d \mod n$

From this two equation we can show RSA encryption and decryption are mutual inverse and commutative. This helps to minimize the resultant hardware area. The original RSA schema is block cipher, original message and cipher message are integer in the interval [0, n-1].propose another schema in which have the original message and encrypted message are h*h square matrices, this method don't have any restriction to encryption and decryption order and its consider as more scalable, efficient and dynamic [15].If we said a computing system is secure, we can trust both hardware and software of that system. In a computing system, if the hardware layer is compromise the security, it's difficult for software to find out that attack is underway. Because of the increasing demand of security in communication channel its necessary to develop a new and efficient hardware security module. Hardware implementation of RSA schema using the modular exponentiation [16] propose for the above security purpose. Along with provide security it's also help to reduce to processing time.

4.1 Security of RSA

RSA consist of public key and private key, public key used for encryption and private key for decryption. Key generation, encryption and decryption this are the soul of RSA algorithm. The security of RSA algorithm is lies on integer factorization problem. So the key selection is very importantIn RSA generally said select a strongest key pair p and q to generate modulus n. the condition of selection of p and q is both numbers are must be prime numbers. Strongprime numbers have certain property. Its provide difficulty to factor n by using any specific factoring method (n=p*q). Public key or encryption key (e, n) is known to everyone, 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 numbers must be efficient. This is the main feature of RSA. The key size decides the strength of the cryptosystem. The size of RSA key typically refers to the size of n. if p and q has larger size numbers 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 but slower the RSA operation.

Attacks against RSA

1. common modulus
2. small encryption exponent "e"
3. small decryption exponent "d"
4. timing attack
5. factoring the public key

4.2 Key generation in RSA

RAS key generation is very complex and time consuming process. It's have following steps

1. select two large prime numbers p and q
2. calculate the modulus totient $\Phi(n)=(p-1)*(q-1)$
3. select public exponent an integer e such that $1<e<\Phi(n)$ and gcd $(e, \Phi(n)) =1$
4. calculate private exponent d such that $d=e^{-1} \mod \Phi(n)$
5. private key is (d,n)
6. public key is (e,n)

RSA working is on the basis of multiplication of two prime numbers, so the number factoring is the serius threating against RSA [17]. Present a novel architecture to provide high processing speed to RSA key generation for embedded platform with limited processing capacity [18].this implementation is based on TTA

(transport triggered architecture) to at the architeural level. Reduce number system (RNS) introduce to achieve more data parallelism and its help to accelerate key generation. By introducing RNS this two independent things can be processed simultaneously. To improve performance RNS adopt both sieve function and primarily test. Develop a new software by using c# to speed up the implementation of the RSA algorithm during data transitionbetween the different communicationsnetworks [19]. Using this software the keys are generated offline and stored different data base. RSA algorithm is computationally intensive when it's operating with very large integers. One way to solve this problem is to apply cryptographic hardware. Present an efficient implementation technique on RSA cryptosystem by using HDL based hardware design methodology and standard algorithms [20].

Elliptic curve isapplicable not only in cryptography but also in prime test and large integer factorization.Combine the true prime test with elliptic curve to develop good primality test on windows platform [21].Prime finding procedure in RSA is most costly part its include two functions randomly selection of numbers and prime test for accuracy. Modular exponentiation is the most computing operation of primality test. To speed up the operation binary method for exponentiation is used and provides a prototype for fast prime finding algorithm. This help to fast implementation of RSA on smart card with crypto-processer [22]. hard ware based true random number generator(TRNG) used for generating random number and Fermat's theorem is used for the primality test to provide secure and fast key generation of RSA on smart card[23]. Pre-defined Fermat's number is used as public keys.Apply both Fermat's and miller Rabin theorem on the RSA in embedded system [24]. Great time complexity is the greatest imperfection in this area.so, to reduce the time complexity proposes an optimization algorithm to generate large numbers.an efficient method for generating large prime numbers is reduce the time required for generating key pair [25].RSA is based on arithmetic modulo which lead to slow in rsa decryption. The encrypt assistant multi prime rsa (EAMRSA) increase the rsa decryption by reducing modulus and private exponent [25]. Introducing a fast and efficient primality testing algorithm on FPGA with the implementation of 64-bit RSA encryption [26]. Using leaner feedback shift register (LFSR), generate the random numbers and apply primality test which is implemented using miller Rabin primality test.Generation of prime numbers include selecting a number and apply prime test. To reduce time space complexity introduce a pre-screen algorithm and after that applying miller-Rabin algorithm for prime test. [27] Pre-screen algorithm is used to improve the efficiency of prime test. Private and public key is generated by using stain algorithm.

4.3 Primality test

In public key cryptosystem, like RSA primality test and integer factorization have an important role. Primalitytest is an algorithm used to determine whether the input number is prime or not. Mainly two kinds prime test algorithm, one is probabilistic prime test and other one is true prime test. Probable prime test is very fast and simple. To get an accurate result this test is done repeatedly. Most common probabilistic prime test is ferma, miller-Rabin, and solovay-strassen tests. True prime test is considerably more accurate, because of its time consuming calculation it's not useful in practical application.Pierre de Fermat is famous mathematician in 17^{th} century. According to Fermat's little theorem if p is any prime number, and$a$ is a natural number, a and$p$ is should be co-prime then $a^{p-1}=1$ (mod p). we already discuss the problems related to RSA algorithm, solution of that problem is find out an effective method for selecting prime numbers while it's a large size. by applying Fermat's theorem during key generation process it help to reduce the time complexity of that process.by applying Fermat's theorem as prime test its help to provide fast key generation on RSA[23][24].

V. RSA ALGORITHM AND CLOUD COMPUTING

Rsa is the most powerful and secure algorithm in present time and it's mainly applicable for network security. Apply RSA algorithm along with digital signature for provide cloud data security [28]. Digital signature is a mathematical schema used for demonstrating the authenticity of the document. If a receiver receive a valid digital signature it's gave a reason to believe the recipient the message is send by a known sender and the message is not altered. "Message digest" is produce by applying hashing function to the original document, digital signature is produce by encrypt this message digest using any encryption software [29].the resultant of this process called digital signature and finally apply RSA algorithm on that and send the cipher text.at receiver side by using RSA private key decrypt the message and public key is used for signature verification.in cc the resources can be access by using any devices, but the most mobile devices cannot process the large size of data if the data to send under encryption method. RSA Signature protocol [30] helps to reduce the loading of computing. Cloud services and users are interacting through a set of software interfaces or API. Insecure API and interfaces are leads to the security problems. To achieve a secure cloud frame work, provide a java based architecture which considers to both client side and admin side security [31].RSA algorithm and MD5 are the underlying concept of the above work. Users upload their encrypted data on the cloud environment through a verification process. Data encryption and decryption is held by using RSA. The admin can decrypt the

data only the read mod, if admin wish to update the user data he need another secret key from users. The user develop second secrete key using MD5 algorithm. To ensure security in Google App engine implement RSA algorithm using cloud SQL [32][33].Implement the RSA algorithm before data storing on cloud. If the authorized user request for the encrypted data then data is decrypted and provide to the user. This way provides protection to the data stored on Google cloud environment. A new technique named as multi finger security model, use three finger templates of users during registration time [34]. Assign a single digit number to each fingers and it's encrypted by using RSA. The templates of the finger print is encrypted by using elliptical algorithm and stored at cloud provider side. Finally check matching of the finger prints and numbers. [35]They apply simple RSA algorithm into the cloud environment by using RSA algorithm only the concerned user can access the encrypted data to provide security.

VI. PROPOSED METHOD

The first condition of RSA algorithm is selection two prime numbers. the products of thisnumber is the part of public and private key.so the selection of p and q is very important and the security of entire system lies on how it's difficult to factor for find out p and q.if the value of n gets larger ,the integer factorization problem gets harder to solving became is larger when we select p and q is large key size number. For the security reason select p and q are key length of 2048bit. Majority time of key generation process is taken for generating large prime numbers [24].therefore its need to optimization of key generation. When a generating a prime number, the prime test is very important. But in the case of large key size number it's difficult to prime test. Its take more time for do that. to reduce the complexity of this process and save time, apply Fermat's little theorem. By applying this theorem, can reduce the key generation time and complexity of the process. Furthermore increase the reliability of the encryption.

VII. CONCLUSION

Cloud computing is the latest trend in IT. But security is the biggest challenge in this area. so, researchers mainly concentrate 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 techniques 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's is the one of the best and strongest encryption method. In RSA key size 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 powerfull.but,the main problem of RSA is increasing key generation time when we select large key size numbers, the key generation time is also increase, this problem can be solved by applying Fermat's little theorem during key generation process. This new method helps to trust users in cc environment. It also reduces the drawback of RSA encryption. So it is faster and better method.

Table 1.Key Generation Time Before And After Using Fermat's Little Theorem （ The System Clock Is 60mhz)[24].

Bits	1024	2048
Before(s)	2.780	9.620
After(s)	2.129	6.896

REFERENCES

[1] YashpalsinhJadeja, KiritModi,cloudcomputing-concepts,architecture,challenges, *International Conference on Computing, Electronics and Electrical Technologies,vol.1*,pp.877-880,2012

[2] Sameer Rajan, ApurvaJairath Cloud Computing: *The Fifth generation of Computing ,International Conference onCommunication Systems and Network Technologie*s IN 2011

[3] florin ogigau-neamtiu, Cloud Computing Security Issues, *journel of defense resource management.vol.3,issue 2(5)*,pp 141-148,2012

[4] PeeyushMathur, Nikhil Nishchal, Cloud Computing: New challenge to

[5] the entire computer industry, 2010 *1st International Conference on Parallel, Distributed and Grid Computing* (PDGC - 2010).

[6] Kuyoro S. O, Ibikunle F, Awodele O, Cloud Computing Security Issues and Challenges,*International Journal of Computer Networks, Volume (3),Issue (5*),pp 247-255, 2011

[7] Simarjeet Kaur, "cryptography and encryption in cloud computing",VSRD international journal of computer science &information technology,vol.2(3),pp.242-249,2012

[8] Ashutosh Kumar Dubey , Animesh Kumar Dubey , MayankNamdev, Shiv Shakti Shrivastava,

[9] Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment, *Software engineering CSI 6th international conference*(page:1-8,year:2012 ISBN: 978-1-4673-2174-7)

[10] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica, A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment, *International Journal of Computer Applications (0975 – 8887) Volume 12– No.8*, December 2010,pp.19-23)

[11] SameeraAbdulrahmanAlmulla, Chan YeobYeun, Cloud Computing Security Management*Engineering Systems Management and Its Applications* (ICESMA), 2010 Second International Conference on , vol., no., pp.1,7, March 30 2010-April 1 2010,ISBN 978-9948-427-14-8

[12] VeerrajuGampala, SrilakshmiInuganti, Satish Muppidi,,Data security in cloud computing with elliptic curve cryptography,*international journal of soft computing engineering,vol.2,isssu.3,*pp.138-141,2012

[13] Mahatebaa,said el hajji,abdellatif el ghazi,homomorphic encryption applied to the cloud computing security,*proceeding of the world congress on engineering*(year of publication:2012 ISBN: 978-988-19251-3-8)

[14] Birendragoswami,dr.s.nsingh,enhance security in cloud computing using public key cryptography with matrices, *International Journal of Engineering Research and Applications,vol.2,issu.4*,pp.339-344,2012

[15] Sherif El-etriby, Eman M. Mohamed,Modern Encryption Techniques for Cloud Computing,*proceedings of the informatics and systems 8th international conference*(page:cc-1-cc-6 year :2012 ISBN: 978-1-4673-0828-1)

[16] Mandeep Kaur, Manish Mahajan, Using encryption Algorithms to enhance the Data Security in Cloud Computing, *International Journal of Communication and Computer Technologies,Vol.12, Issu.3*,pp 56-59,2013

[17] Sattar J Aboud1, Mohammad A AL-Fayoumi1, 2Mustafa Al-Fayoumi and 3Haidar S Jabbar,An Efficient Rsa Public Key Encryption Scheme,*5th international conference on Information Technology: New Generations*(page 127-130, year 2008,ISBN 0-7695-3099-0)

[18] Muhammad I. Ibrahimy, Mamun B.I. Reaz, KhandakerAsaduzzaman and SazzadHussain,FPGA Implementation of RSA Encryption Engine with Flexible Key Size,*international journal of communications,vol.1,isuue.3*,pp.107-113,year 2007

[19] Majid Bakhtiari ,MohdAizainiMaarof ,Serious Security Weakness in RSA Cryptosystem, *International Journal of Computer Science Issues,Vol. 9, Issue 1*, No 3, pp.175-178,January 2012

[20] Vishak M1 &N.Shankaraiah, Implementation Of Rsa Key Generation Based On Rns Using Verilog, *International Journal of Communication Network Security,vol.1,issu.4*,pp 12-16,2012

[21] Sami A. Nagar and SaadAlshamma,High Speed Implementation of RSA Algorithm with

[22] Modified Keys Exchange, *6th international conference on Sciences of Electronics, Technologies of Information and Telecommunications*, (pp.639-642,year. 2012,ISBN978-1-4673-1657-6)

[23] Mostafizur Rahman, Iqbalur Rahman Rokon and Miftahur Rahman, Efficient Hardware Implementation of RSA Cryptography,*3rd international conference on Anti-counterfeiting, Security, and Identification in Communication*,(pp.316-319,year 2009,ISBN. 978-1-4244-3883-9)

[24] Chung-Huang Yang, Chun-ChihPeng,Design and Implementation for Integer Factorization and Primality Testing Tools with Elliptic Curve on Windows Platforms,*The 2007 Symposium on Cryptography and Information Security Sasebo*,pp 23-26,year.2007

[25] ChenghuaiLu,Andre L. M. dos Santos,Francisco R. Pimentel,Implementation of Fast RSA Key Generation on Smart Cards,*Proceedings of the 2002 ACM symposium on Applied computing*, year march 2002,pp.214-220

[26] Milad Bahadori1, Mohammad Reza Mali, OmidSarbishei, MojtabaAtarodi, Mohammad Sharifkhani,A Novel Approach for Secure and Fast Generation of RSA Public and Private Keys on SmartCard, *NEWCAS Conference* (NEWCAS), 2010 8th IEEE International,(pp.265-268,year.2010,ISBN. 978-1-4244-6804-1)

[27] Li Dongjiang,WangYandan,an optimization algorithm of RSA key generation in embededsystem,*journal of theoretical and applied information technology,vol.46*,pp.84-87,2011

[28] p.saveetha1 & s.arumugam2,Study On Improvement In Rsa Algorithm And Its Implementation, *International Journal of Computer & Communication Technology,vol.3,issu.6*,pp 61-66,year 2012

[29] Rehan Shams ,FoziaHanifKhan,UmairJillaniand,M. Umair, Introducing Primality Testing Algorithm with an Implementation on 64 bits RSA Encryption Using Verilog,*SSU Res,vol.2,issue.1*,pp.12-17,year.2012

[30] Li Dongjiang, Wang Yandan, Chen Hong,The research on key generation in RSA public- key cryptosystem,*Fourth International Conference on Computational and Information Sciences*,(page.578-580,year:2012,

[31] Esh Narayan, Mohit Malik, AmanPreet Singh, PremNarain,To Enhance The Data Security Of Cloud In Cloud Computing Using Rsa Algorithm*Bookman International Journal of Software Engineering, Vol. 1*,pp 8-11,Sep. 2012

[32] Uma Somani, 2 Kanika Lakhani, #3 Manish Mundra, Implementing Digital Signature with RSA EncryptionAlgorithm to Enhance the Data Security of Cloud in Cloud Computing, *1st International Conference on Parallel, Distributed and Grid Computing*(page:211-216 year of publication 2010 ISBN: 978-1-4244-7675-6)

[33] Chu-Hsing Lin, Chen-Yu Lee, and Tang-Wei Wu,A Cloud-aided RSA Signature Scheme for Sealing and Storing the Digital Evidences in Computer Forensics,*International Journal of Security and Its Applications Vol. 6, No.* 2, pp-241-244, April, 2012

[34] Ashutosh Kumar Dubey ,Animesh Kumar Dubey , MayankNamdev, Shiv Shakti Shrivastava, Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. *Software engineering CSI 6th international conference* (page:1-8,year:2012 ISBN: 978-1-4673-2174-7)

[35] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam,An Implementation of RSA Algorithm in Google Cloud using Cloud SQL,*Research Journal of Applied Sciences, Engineering and Technology,vol.4(19),*pp 3574-3579,2012

[36] Vijeyta Devi &VadlamaniNagalakshmi,"A Prospective Approach On Security With Rsa Algorithm And Cloud Sql In Cloud Computing, *International Journal of Computer Science and Engineering,vol.2,issue.2*,pp35-44,2013

[37] D.Pugazhenthi,B.SreeVidya**, "** Multiple Biometric Security in Cloud Computing,*International Journal of Advanced Research in Computer Science and Software Engineering,vol.3,isssue.4*, pp.620-624,2013.

[38] 35.ParsiKalpana, SudhaSingaraju,Data Security in Cloud Computing using RSA Algorithm, *International Journal of Research in Computer and Communication technology, Vol .1, Issue. 4*, pp.143-146,2012.