A Simplified Data Security Aspect In Cloud Computing – "Modified RSA Implementation"

Uma Naik, V. C. Kotak
Department of Electronic Engineering,
SAKEC, Mumbai

***Abstract*— Security can only be as strong as the weakest link. In this world of secrecy, it is now well established, that the weakest link lies in the implementation of security algorithms. This paper deals with RSA algorithm implementation with increased number of exponents for more security. This paper deals with security implementation in cloud for defending cloud infrastructure against various attacks, where RSA algorithm can be used for security point in cloud.**

***Index Terms*— RSA algorithm, security exponents, secrecy, encryption, decryption, data security, cryptography.**

I. INTRODUCTION

Organizations in both public and private sectors have increasingly dependent on electronic data processing. Protecting these data is of utmost concern to the organizations and cryptography is one of the primary ways to do the job. Cryptography, defined as the science and study of secret writing concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message. Security often requires that data be kept safe from unauthorized access. And the best line of defence is physical security (placing the machine to be protected behind physical walls). However, physical security is not always an option, due to cost and/or efficiency considerations. Instead, most computers are interconnected with each other openly, thereby exposing them and the communication channels that they use.

II. CLOUD COMPUTING

Cloud Computing is a set of IT based Services that are provided to a customer over a network and these services are delivered by a third party provider who owns the infrastructure. It is often provided "as a service" over the Internet and that was typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), data storage as a service (DSaaS). [6][12]

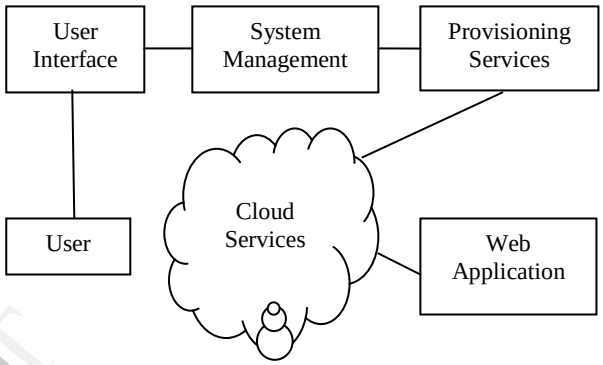


Figure 1: Cloud System

Interest in the cloud is growing because cloud solutions provide users with access to super computer like power at a fraction of the cost of buying such a solution outrights. More importantly, these solutions can be acquired on demand, the network becomes the supercomputer in the cloud where users can buy what they need when they need it. Cloud computing identifies where scalable IT- enabled capabilities are delivered as a service to customers using Internet technologies.[4][19]

III. PROBLEM ANALYSIS

External attacks, unauthorized access, threads breaks sensitive data.[2][5]

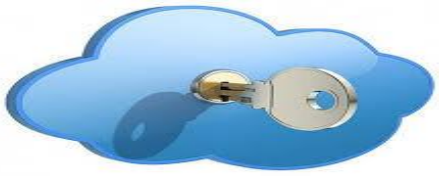


Figure 2: Security Of cloud storage

To defend cloud infrastructure against malicious attacks, this paper associates with design & implements the security

IV. Blocks Of Cloud COmputing

Cloud computing is actually a combination of various computing techniques like virtualization, distributed computing, load balancing etc. [7]

The building blocks of cloud computing are as follows:[1][2][5][12]

A. Deployment Models
- Private Cloud
- Public Cloud
- Community Cloud
- Hybrid Cloud

B. Delivery Models
C. Hallmarks of Cloud
D. Service Models
- Software As A Service (SAAS)
- Platform As A Service (PAAS)
- Infrastructure As A Service (IAAS)

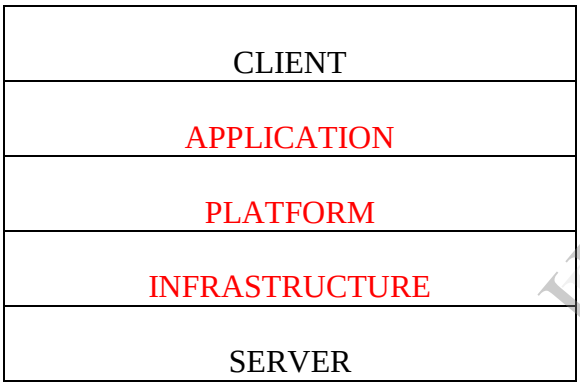


Figure 3 : Layers Of Cloud Storage

V. Security Issues & Challenges [1][8]

A. Trust
B. Privacy
C. Security
D. Ownership
E. Performance and Availability
F. Legal
G. Multiplatform Support
H. Intellectual Property
I. Data Backup
J. Data Portability and Conversion

VI. Security Algorithms For Cloud

Different security algorithms of data security are as follows –[3][12]

Symmetric Algorithm

- DES
- AES

Asymmetric Algorithm
- RSA

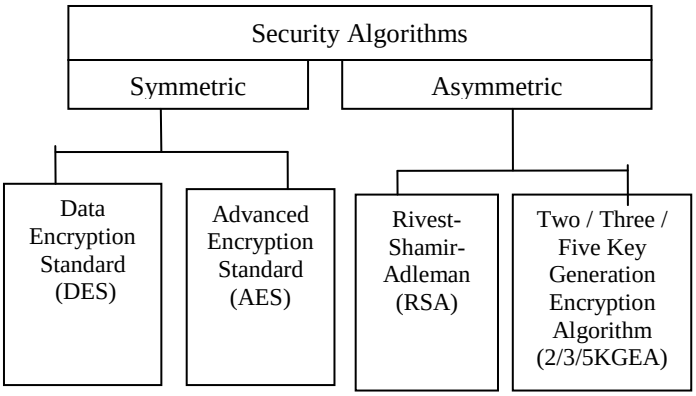


Figure 4 : Security Algorithms

The simplest out of these is RSA which is been implemented with following RSA algorithm. RSA taken into consideration for further development and implementation of increased security aspects with increased exponents as proposed schema[3][12]

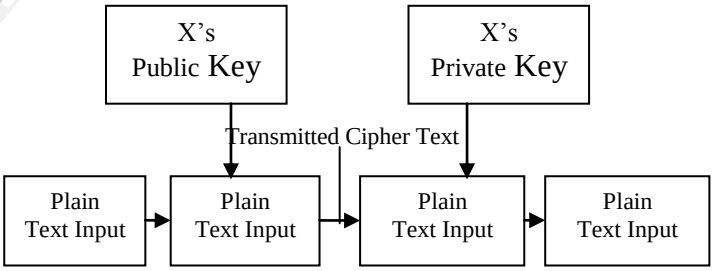


Figure 5:Security - Encryption & Decryption Process

The security of RSA algorithm depends on the ability of the hacker to factorize numbers. New, faster and better methods for factoring numbers are constantly being devised. The Trent best for long numbers is the Number Field Sieve. Prime Numbers of a length that was unimaginable a mere decade ago are now factored easily. Obviously the longer a number is, the harder is to factor, and so the better the security of RSA. As theory and computers improve, large and large keys will have to be used. The advantage in using extremely long keys is the computational overhead involved in encryption / decryption. This will only become a problem if a new factoring technique emerges that requires keys of such lengths to be used that necessary key length increases

much faster than the increasing average speed of computers utilizing the RSA algorithm. RSA's future security relies solely on advances in factoring techniques.

VII. RSA IMPLEMENTATION

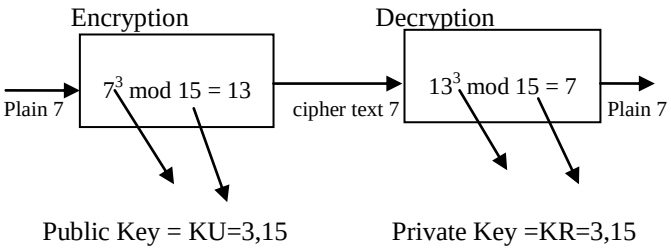
The original RSA algorithm was publicly known in 1977 and after that many similar algorithms were designed based on original RSA in order to overcome the weaknesses of the basic algorithm. RSA names in honour of Rivest, Shamir and Adleman for their realisation of public key crypto and signing systems.[6][9][16]

A] Key Generation Algorithm
B] Encryption Process
C] Decryption Process

The most important advantage of RSA is ensuring the privacy of the private key because this key will not be transmitted or revealed to another user. The computational costs of the RSA are modular exponentiations found during key generation, encryption and decryption process. Various simple ways are now been implemented to simplify the complex calculations of exponents for quick and verified results. [6][12]

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}
Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure 6 : Basic RSA Algorithm



Public Key = KU=3,15 Private Key =KR=3,15

1. Select primes : $p = 3$ & $q = 5$
2. Compute $n = p.q = 3\times5 = 15$
3. Compute $\phi(n) = (p-1).(q-1) = 2\times4 = 8$
4. Select e *:* gcd(e,8) = 1; choose $e = 3$
5. Determine d*:* $d.e = 1 \bmod 8$ and $d < 8$ Value is d = 3
6. Publish public key KU = {3, 15}
7. Keep secret private key KR = {3,15}

- sample RSA encryption/decryption is:

given message M = 7 (such that M<n)

encryption: $C = M^e \bmod n = 7^3 \bmod 15 = 13$

decryption: $M = C^d \bmod n = 13^3 \bmod 15 = 7$

Figure 7 : Existing RSA Algorithm – Example Implemented

VIII. PROPOSED RSA ALGORITHM

This has weakness against certain attacks such as Brute force, mathematical attacks, timing attacks and cipher text attacks. For this to overcome RSA small-e and Efficient RSA are popular algorithms which improves the main algorithm. So the three / five Key Generation Encryption (3KGEA/5KGEA) is the proposed schema, where the number of exponents will be increased to 3 minimum and 5 maximum, for now.[11][14][17]

This proposed algorithm will be suggested in cloud computing environments. Only the time and memory aspects due to sharing effects of resources needs to be checked. May be an symmetric and asymmetric key algorithms used in sharing actions. The name 5KGEA can be further modified as per the results and judgements of final implemented proposed algorithm appears to be better in terms of time , simplicity, and security for dual and triple actions of getting known to third party in transit.[11][13][15][18]

1. Select primes : $p = 3$ & $q = 5$
2. Compute $n = p.q = 3\times5 = 15$
3. Compute $ø(n) = (p–1)(q-1) = 2\times4 = 8$
4. Compute z =abs[(p- $ø(n)$)- (q- $ø(n)$)]

   = (3-8)-(5-8) = 2
5. Compute w = abs[(p-z)+(q-z)] = (3-2)+(5-2) = 4
6. Select r *:* gcd (r,15) = 1; choose $r = 3$
7. Determine e : r.e=1 mod 8 , value of e = 3
8. Determine d *:* $d.e = 1$ mod 2 and $d < 15$ value is d = 1
9. Determine h : h.d = 1 mod 2, value is h = 3
10. Determine j: j.e = 1 mod 8, value is j = 3
11. Publish public key KU = {e,j,n} = {3,3,15}
12. Keep secret private key KR = {r,d,h,n} = {3,1,3,15}

- sample RSA encryption/decryption is:

  given message M = 3 (such that M<n)
  encryption: E = M*e mod n = 3*3 mod 15 = 9
  = E^j mod n = 9^3 mod 15 = 9

  decryption: M = E*r mod n = 9*3 mod 15 = 12
  = M^h mod n = 12^3 mod 15 =3
  = M*d mod n = 3*1 mod 15 = 3

Figure 8 : Existing 5 exponent RSA Algorithm - Example Implemented

OUTPUT RESULT

Five exponent proposed RSA Algorithm – 5KGEA Method been implemented

Enter the value of p: 3
Enter the value of q: 5
value of n : 15
value of phi : 8
value of z : 2
value of w : 4
enter prime number less than n: r= 3
value of e : 3
value of d : 1
value of h : 3
value of j : 3
the public key are: {3,3,15}
the private key are: {3,1,3,15}
Enter the message: M=3
Encrypted Message 9
Decrypted Message 3

IX. CONCLUSION

The existing algorithms of symmetric key and public key cryptography are studied in detail and implemented using platforms like C++ and Matlab. A complete package which includes all the algorithms was developed. The technique using self-repetitive concept was successfully implemented in MATLAB. A communication channel was successfully modeled which used proper decompression techniques for effective communication. The numerical method suggested to find N value of a matrix was successfully tested and used in the implementation. It was found to be easier to compute and simpler to implement and difficult to crack.

In this paper, proposed is implementation of security with RSA, implementing intrusion tolerance via RSA cryptography. Performance analysis shows that its highly efficient & resilient against malicious data modification attack.

Basic RSA algorithm for security issue handling in cloud computing is been implemented. Moreover, a hybrid asymmetric key encryption algorithm like 2KGEA / 3KGEA / 5KGEA based on RSA small-e and Efficient RSA for security issues in cloud computing environment with execution time to be increased than original RSA

X. FUTURE WORK

3KGEA /5KGEA algorithm to be implemented further for better and faster execution with more reliable security provided. Implementation of RSA done in C program and make system usage simple and more reliable. Proposed schema to be implemented for better data security results as a further more security parameters to the existing exponents and the algorithm.

Further actual cloud applications based on this algorithm been implemented and others like cloud instrumentation will be taking boom in field of computer science.[10]

REFERENCES

[1] Cloud Security and Privacy . An Enterprise Perspective - Tim Mather, Subra Kumaraswamy
[2] Cloud Computing - Web Based Applications That Change the Way You Work and Collaborate Online - Michael Miller
[3] Cryptography and Network Security – Behrouz A. Forouzan and Debdeep Mukhopadhyay.
[4] Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing - Cong Wang, Qian Wang, and Kui Ren Department of ECE, Institute of Technology, - Wenjing Lou Department of ECE, Worcester Polytechnic Institute. (Review Paper at direction of IEEE communications society – IEEE INFOCOM 2010)

[5] On Technical Security Issues In Cloud Computing - Meiko Jensen, Jorg Schwenk (Germany) and Nils Gruschka, Luigi Lo Lacono (NEC Europe Ltd.). (2009 IEEE International Conference on Cloud Computing)
[6] To Enhance the Data Security Of Cloud in Cloud Computing using RSA Algorithm – Esh Narayan, Mohit Malik, Amar Preet Singh, Prem Narain. (Research Scholar, Dept Of Computer Application, UP, India) - Research Article
[7] Providing Privacy Preserving in Cloud Computing - Jian Wang, Yan Zhao, Shuo Jiang, Jiajin Le, College of Information Science and Technology, Donghua University Shanghai, china. (2009 International Conference on Test and Measurement).
[8] A review on cloud computing security issues & challanges - F. A. Alvi, B.S Choudary, N. Jaferry, E.Pathan, Department of Computer Systems Engineering and Electronic Engineering, QUEST Nawabshah, Sindh, Pakistan
[9] Developing an application of RSA algorithm with Java – M. Nusret Sarisakal, Selcuk Sevgen, Dogal ACAR Istanbul University, Faculty of Engg, Department of Computer Engg, 34850, Avcilar, Istanbul, Turkey.
[10] Cloud Instrumentation,' the instrument is in the cloud' – Marius Ghercioiu President of Tag4M at Cores Electronic LLC (Austin, TX, USA)
[11] An improved RSA Encryption Algorithm for Cloud Computing Environments : Two Key Generation Encryption (2KGEA) – Ms Shubhra Saggar, Dr. R.K.Datta, Research Scholar, Singhania University. International Journal of Software and Web services (IJSWS), International Association of Scientific Innovation and Research (IASIR).
[12] Cloud Computing : Security Issues and Description of Encryption Based Algorithms To Overcome Them – Leena Khanna, Prof Anant Jaiswal. International Journal of Advanced Research in Computer Science and Software Engg. - Research Paper.
[13] Implementation Of Data Security in Private Cloud, *S.W.Wasankar, Dr.P.R.Deshmukh, C.O.E.T Amravti, Maharashtra (MS), International Journal of Computer Science and Management Research Vol 2 Issue 4 April 2013, ISSN 2278-733X
[14] Efficient Implementation of RSA Algorithm with MKE, Sami A. Nagar and Dr. Saad Alshamma, Sudan university of Science and Technology Electronic Engineering College / Department of Communication - Khartoum – Sudan
[15] The Mathematics of the RSA Public-Key Cryptosystem Burt Kaliski RSA Laboratories
[16] Data Security Using RSA Algorithm In Matlab, Shikha Kuchhal , B.E, M Tech (ECE), Research Scholar , Ishank Kuchhal , B Tech, M Tech Scholar
[17] Security Algorithms in Cloud Computing :Overview , M. Vijayapriya M. Phil. Research Scholar, PG & Research Department of Computer Science, Government Arts College, Coimbatore-18. M. Vijayapriya / International Journal of Computer Science & Engineering Technology (IJCSET)
[18] Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing
Mohit Marwaha1, Rajeev Bedi2 1 Computer Science And Engineering, Punjab Technical University, Beant College of engineering and Technology Gurdaspur, Punjab, India
Computer Science And Engineering, Punjab Technical University, Beant College of engineering and Technology Gurdaspur, Punjab, India
IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013
[19] Online Technical Support based on Google, Cloud Companies and other search engines.