Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

Cloud Data Security with Modified RSA Algorithm

A Arjuna Rao[1], P Praveen Kumar[2], K Sujatha[2],
S Siva Prathyusha[3], Rahul Singh[3]
[1] Professor & Director, Miracle Educational Society Group of Institutions,
Bhogapuram, Vizianagram, India
[2] CSE Department, Miracle Educational Society Group of Institutions, Bhogapuram, Vizianagram, India
[3] B.Tech. Student, CSE Department, Miracle Educational Society Group of Institutions , Vizianagram

***Abstract*— Cloud provides the means that to instantly use new services and expand the infrastructure. But lack of physical management, bring a full host of cloud security problems and arises issues like information deletion, leakage. Encoding of knowledge held on in cloud permits finding these problems. RSA algorithmic program is public key encoding algorithmic program planned by Rivest-Shamir-Adleman. This has been used for years thanks to its simplicity and security. Modified RSA algorithm is proposed here to boost the safety of RA algorithmic program. Cuckoo Search algorithm is that the improvement algorithmic program that's wont to choose the random values employed in RSA algorithmic program. This can be supported biological facts wherever Cuckoo Birds selects the nests of different birds to put the eggs. Cloud information Security is provided by victimization this hybrid algorithm. This proposed methodology provides increased security and effectively uses the algorithm. Checking results are simulated that proves that the developed program provides reliable confidentiality.**

***Keywords:* cloud security issues, Authentication, data deletion, leakage, Encryption, RSA Algorithm, Rivest-Shamir-Adleman, Modified RSA, Cloud Data Security.**

I INTRODUCTION:

The advancements of cloud computing has drastically altered everyone's view of infrastructure architectures, development models and software system delivery. Sticking as associate degree organic process step, following the transformation from mainframe computers to client/server models. This speedy transformation towards the clouds, has fuelled considerations on a critical issue for the success of communication, knowledge system and knowledge security. From a security view, variety of uncontrollable risks and challenges are presented from this transfer to the clouds. Cloud computing security refers to the collection of process, procedures and standards developed to produce data security guarantee in a cloud computing atmosphere.

Cloud computing security reports every physical and logical security issues across all the numerous service models of platform, infrastructure, and software systems. It additionally reports however these services area unit delivered non-public, public or hybrid model. Cloud security experiences a broad change of security constraints from end-user, associate degree and cloud provider's view, whenever the end-user can predominately are engaged with the provider's security policy, wherever and however their information is keep and agency has access thereto information. For a cloud supplier, on the other side, cloud pc security problems will differ from the physical security of the infrastructure and therefore the access management method of cloud assets, to the execution and maintenance of security policy terms. Cloud security is very important as a result of its most likely the most important reason why organizations worry the cloud. Cloud encoding will be used within the Cloud Security entry that acts to safeguard information – each at rest and within the cloud – from unauthorized access. Learn a lot of concerning cloud encryption.

Cloud information Security will be achieved through watching and news on cloud use via a management console that enables users to outline and maintain information discovery, analysis and protection policies. The Cloud Security Alliance (CSA), a non-profit-making organization of business specialists, has developed a pool of pointers and frameworks for implementing and implementing security at intervals a cloud operative surroundings.

Problems identified in Cloud Storage

- Data will be purloined
- Information is victimized
- Unauthorized access
- Modification of content
- Secured information is attacked

II CLOUD DATA STORAGE USING MODIFIED RSA

By using Hybrid RSA and CS algorithmic rule Security may be provided to the information hold on in Cloud. This maintains the confidentiality and integrity in knowledge that's hold on in cloud. Unauthorized users cannot access the contents that are placed in cloud. The information present in it cannot be altered or changed as this is often not understood by them.

2.1 Cuckoo Search Algorithm:

Cuckoo Search is associate improvement formula proposed by Xin-she principle and Suash Deb in 2009. it had been

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

galvanized by the obligate brood paratism of some cuckoo species by placing their eggs within the nests of different host birds (of different species).Some of the host birds will have interaction direct conflict with the intrusive cuckoos. As an example, if a host bird identifies the eggs aren't their own, it'll either throw these host bird eggs away or just collapses its nest and make a replacement nest elsewhere. Some cuckoo species like the New World brood parasitic Tapera have evolved in such the simplest way that feminine parasitic cuckoos area unit typically terribly specialized within the mimicry in colours and order of these eggs of many chosen host species.

Due to its promising potency in resolution several improvement issues and real world applications are using this concept. Since the primary introduction of Cuckoo Search (CS) by Xin-She principle and Suash Deb female in 2009, the literature of this formula has exploded. Cuckoo search, which has been drawn its inspiration from the brooding paratism of cuckoo species in Nature, were first off projected as a tool for numerical perform improvement and continuous issues. Researchers tested this formula on some well-known benchmark functions and compared with PSO and GA, and it had been found that cuckoo search achieved higher results than the results by PSO and GA.

Since then, the initial developers of this formula and lots of researchers have additionally applied this formula to engineering improvement, wherever Cuckoo search additionally showed promising results. today cuckoo search has been applied in nearly each space and domain of perform.

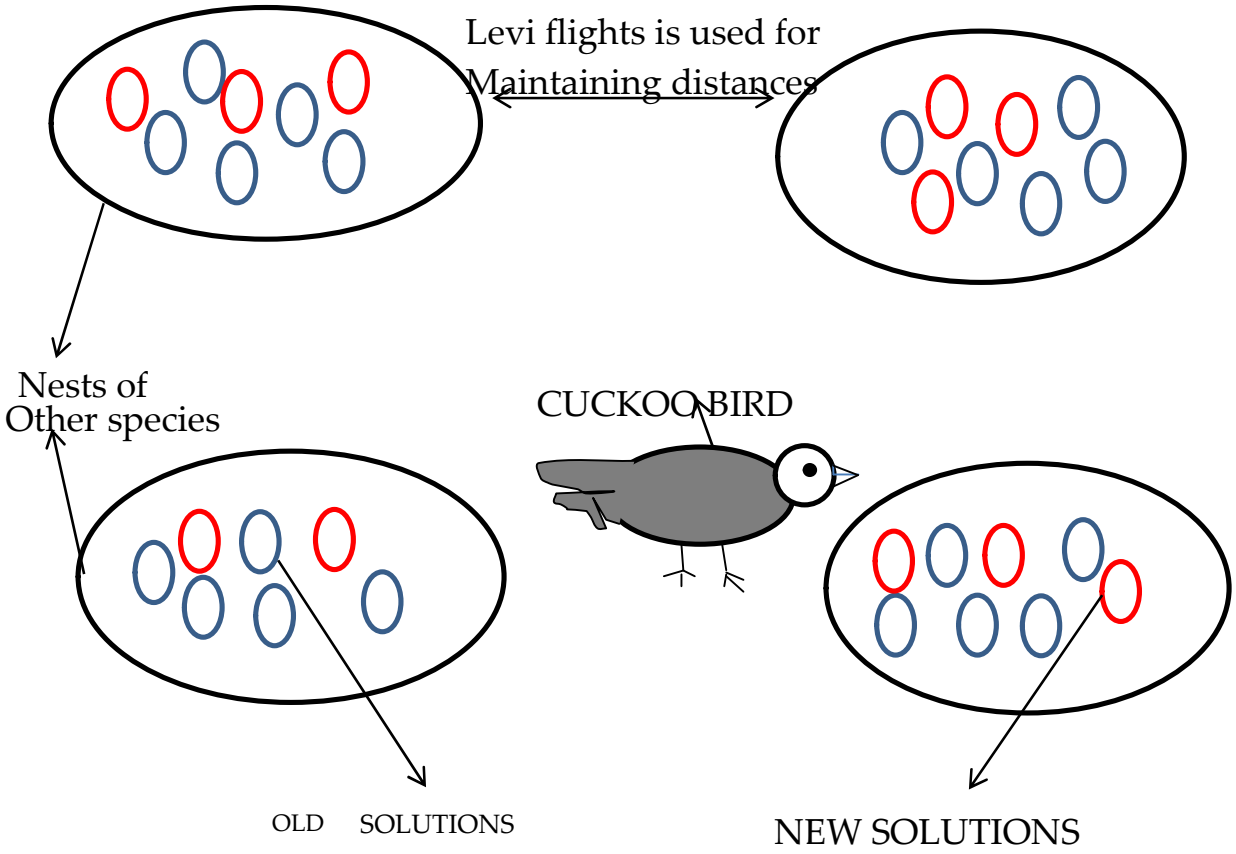


Fig: Cuckoo Search Optimization

Optimization, engineering optimization, image process, scheduling, planning, feature choice, forecasting, and real-world applications. Cuckoo search idealized such breeding behavior, and therefore is applied for numerous improvement issues. It appears that it will outgo different metaheuristic algorithms in applications.

Each egg during a nest signifies an answer, and a cuckoo egg signify a brand new answer. The aim is to use advanced and probably higher answers (cuckoos) to exchange a not-so-good solution within the nests. Within the simplest kind, every nest has one egg. The algorithmic program is extended to additional sophisticated cases within which every nest has multiple eggs signifying a collection of solutions.

Cuckoo Search is based on three rules:
1. At a single a cuckoo can lay one egg at once, and places its egg in a very willy-nilly chosen nest;
2. The simplest nests with prime quality of eggs can carry over to future generation;

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

3. The quantity of obtainable hosts nests is mounted, and the egg placed by a cuckoo is discovered by host bird. Discovering some set of worst nests, and discovered solutions drop from farther calculations.

2.2 Modified RSA

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a scientific discipline algorithmic rule that was primarily to interchange the less secure National Bureau of Standards (NBS) algorithmic rule. Most significantly, RSA implements a public-key cryptosystem, further as digital signatures. RSA is motivated by the revealed works of Diffie and Hellman from many years before, who represented the concept of such an algorithmic rule. This is introduced at the time once the time of electronic email was expected to shortly arise. RSA technique is one among the foremost standard public-key techniques and is foretold on the matter of factorization massive numbers. RSA could be a cryptosystem that supports public-key secret writing. This is often wide used for securing sensitive knowledge significantly once being sent over an insecure network like the web.

Public and the private key-generation calculation is the most complex piece of RSA cryptography. Two expansive prime numbers, p and q, are produced utilizing the Rabin-Miller primality test calculation. A modulus n is ascertained by increasing p and q. This number is utilized by both public and private keys and gives the connection between them. Its length, generally communicated in bits, is known as the key length. People in general key comprises of the modulus n, and an open type, e, which is regularly set at 65537, as it's a prime number that is not very substantial. The figure doesn't need to be a subtly chosen prime number as the general population key is imparted to everybody. The private key comprises of the modulus n and the private type d, which is ascertained utilizing the Extended Euclidean calculation to locate the multiplicative inverse regarding the totient of n.

The Modified RSA algorithm with cuckoo search is as follows.

1. Select large primes p and q using cuckoo search algorithm.
2. n and Ø are calculated by using p and q n= p * q Ø = (p1)*(q-1)
3. Select exponent e is selected basing on n and private exponent d from e, p and q. Here, (n, e) is treated as the public key and (n, d) as the private key.
4. The RSA encryption shown in equation (7) is the exponentiation to the eth power modulo n

$$C = M^e \bmod n \quad - (7)$$

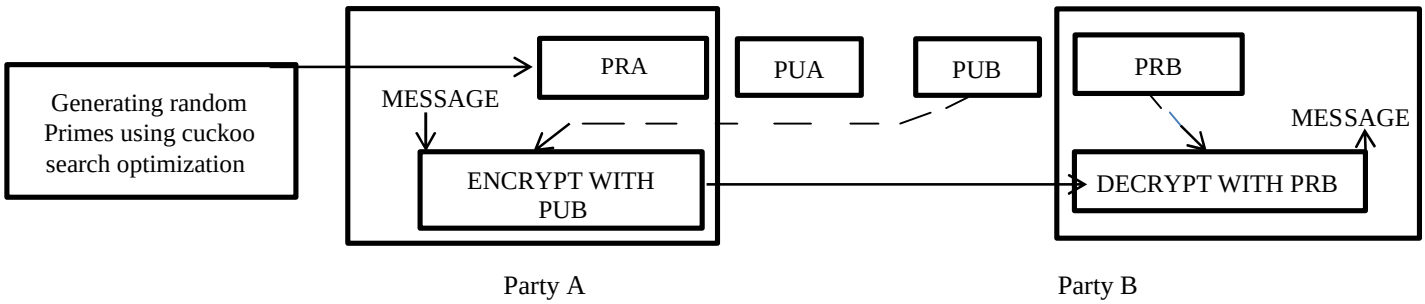
5. The decryption shown in equation (8) is performed as exponentiation to the dth power modulo n

$$M = C^d \bmod n – (8)$$

Encryption of information that is put away in cloud is taken care of by MRSA which is encoded by public key in general key and can be unscrambled just by the client who has the private key. Thus any client who has the mutual public key of indicated client can scramble the information however just the predefined client can decode.

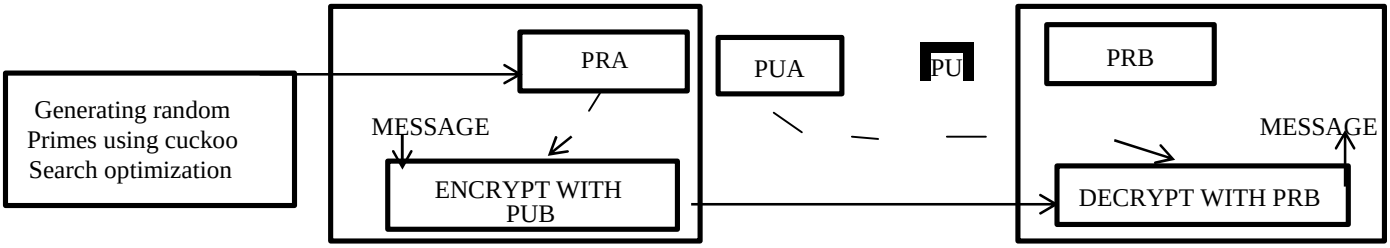
CLOUD DATA SECURITY WITH MODIFIED RSA:

When only confidentiality is needed:



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

When only authentication is needed:



Party A Part B

III RESULT

RSA actualizes idea of public key cryptography. This can make littler, speedier and more productive cryptographic keys. RSA creators indicate that the encryption time per block expands no quicker than the cube of the quantity of digits in n. The secured algorithm is produced and tried utilizing different specimen sets of information and is discovered secure. At that point this is tried on cloud application to give brought together security to cloud[6].

IV CONCLUSION

The issue of security was taken care of by implementing encryption to cloud information security. All the issues in manual framework are solved by utilizing this mechanized encryption framework. This can be utilized as a part of any framework that requires distinguishing the client safely and with dependability. Security is never constrained to an application and hence this calculation can be utilized as a part of numerous related issues which are having such issues.

REFERENCES

[1] Zhang Qing; Hu Zhihua; ―The Large Prime Numbers Generation of RSA Algorithm Based on Genetic Algorithm, Intelligence Science and Information Engineering (ISIE), 2011 International Conference on 20-21 Aug. 2011, pp 434 – 437.

[2] Xin Zhou,Xiaofei Tang, ―Research and implementation of RSA algorithm for encryption and decryption, Strategic Technology (IFOST), 2011 6th International Forum, Vol 2, Aug. 2011, pp 1118 – 1121, IEEE.

[3] Chhabra, A,Mathur, S., ―Modified RSA Algorithm: A Secure Approach, Computational Intelligence and Communication Networks (CICN), 2011 International Conference, 7-9 Oct. 2011, pp Page(s): 545 – 548, IEEE

[4] Elgamal, T., ―A public key cryptosystem and a signature scheme based on discrete logarithms, Information Theory, IEEE Transactions , Jul 1985, Vol 31, Issue: 4,pp 469 – 472, IEEE.

[5] Taher El Gamal. ―A public key cryptosystem and a signature scheme based on discrete logarithms, in Proceedings of CRYPTO 84 on Advances in cryptology, pages 10–18. Springer-Verlag New York, Inc., 1985.

[6] K. Sujatha ; P V Nageswara Rao ; A Arjuna Rao et al.,; Design and development of mobile application for postal department service management, Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference, 24-25 Jan. 2015, pp 1-5, IEEE.