

A Comparative Survey of Algorithm used in Cloud Computing

Roshitha.P.P¹, Nowshad.M.U², T.Sivakumar³

^{1,2}PG Scholar, ³Assistant Professor

^{1,2,3}Department of Computer Science and Engineering

^{1,3}Maharaja Institute of Technology, Coimbatore, India

²Royal College of Engineering and Technology, Akkikkavu, India

roshithapp49@gmail.com¹, nowshad@royalcet.org², sivakumarrts@gmail.com³

Abstract: Cloud computing is emerged as a data interactive model in which users can store their data in an online cloud server. Cloud computing services can be private, public or hybrid. Users can access the applications as utilities over the internet. We can create, configure and customize the application. Online storing and retrieving data in third party's cloud system causes serious conflict over data security and data confidentiality. To overcome this problem, methods like cryptography can be used. The data stored in encrypted format and it will make available to the authenticated requested person after decrypting the data. As the cloud server has numerous amounts of data, load balancing is also a serious concern. Here we have studied and made a comparative analysis of algorithm used in cloud computing for secured data forwarding and load balancing.

Keywords: Cloud Computing, Proxy Re-encryption, Erasure Coding, Cryptographic Splitting, Cloud Storage, Block Cipher, Encryption, Decryption.

1. INTRODUCTION

Cloud computing refers to using a remote servers hosted on the internet to store, manage and process data. It is a shared pool of configurable computing resources. The essential characteristics of cloud computing listed by NIST are on-demand self-service, broad network access, Resource pooling, rapid elasticity, Measured Service. The service models provided by cloud computing are software as a service, platform as a service, infrastructure as a service. The deployment models are private cloud, community cloud, public cloud, hybrid cloud. Encryption algorithm plays as important role in providing security for data forwarding over the network. Encryption algorithm convert the data in the server into scrambled form and the user having the key to decrypt the data can view by decryption method. Only one key is used to encrypt and decrypt the data in symmetric key encryption. In asymmetric key encryption two keys are used as Public key for encryption and private key for decryption. Secured data forwarding can be achieved using proxy re-encryption scheme. PRE scheme allow proxies to alter a cipher text that is encrypted for one party so that it may be decrypted by another one. It is similar to traditional symmetric or asymmetric encryption schemes with addition of two function delegation and transitivity. Identity based security is a network approach that provide control and visibility over user activity as a part of firewall matching criteria. Erasure coding used in cloud, where data's are broken into fragments, expanded, encoded and stored across different locations. The proxy re-encryption scheme supports encoding operation over encrypted data. The encryption of stored data can be done using different algorithms.

1.1 BLOWFISH ALGORITHM

Blowfish is a symmetric cryptographic block cipher. It replaced the DES or IDEA. It is the fastest block cipher in public use. Blowfish has a 64 bit block size and key length ranging from 32 bits to 448 bits. It is a feistel cipher having 16 round. Each time in network represents 32 bits and algorithm keep two subkey arrays, the 18 entry P array and four 256 entry S boxes. One entry of P array is used every round and after final round, each half of data block is XORed with one of the two remaining unused P entries. The F function splits 32 bit input in to four 8 bits quarters and uses the quarters as input to S boxes. The outputs are added modulo 232 and XORed to produce final 32 bit output. When changing the keys each new key requires pre-processing, that is equal to encrypting about 4 kilobytes of text. It is very slow compared to other block ciphers. So it is suitable for products function on mobile phones, notebook, and desktop.

1.2 RIJNDAEL ALGORITHM

Rijndael is the block cipher algorithm chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES). The algorithm is designed to replace the DES algorithm. It is an iterated block cipher. Thus, the encryption or decryption of a block of data is achieved by the iteration (a round) of a specific transformation (a round function). Rijndael generate a series of subkeys from the original key. The subkeys are used as input with the round function. It was designed based on resistance against attacks, Speed, and simplicity. The length of the block to be encrypted and encrypted key is not fixed.it can be specified in 128,192,256 bits. It provides high protection against brute force attacks. The number of rounds varies according to key length. The encryption method works three times faster in software than DES. This method can be used for exchanging keys and transferring data with a size of 128 or 256 bits. The method is based on replacing, changing and performing XOR operations on bytes. The method works as, From the 128-bit key; Rijndael generates 10 keys of 128 bits each. These keys are placed into 4x4 arrays. The plain text is also divided into 4x4 arrays (128 bits each).Each of the 128-bit plain-text items is processed in 10 rounds (10 rounds for 128-bit-keys, 12 for 192, 14 for 256).After the 10th round the code is generated. Each single byte is substituted in an S box and replaced by the reciprocal on GF (2 8).Then a bit-wise modulo-2 matrix is applied, followed by an XOR operation with 63.The lines of the matrices are sorted cyclically. The columns of the matrix multiplication are interchanged on GF (2 8).The subkeys of each round are subjected to an XOR operation.

1.3 DATA ENCRYPTING STANDARD (DES) ALGORITHM

DES is a symmetric key block cipher. It uses 16 round feistel structure. The block size is 64 bit. 64 bit plain text goes as inputs which produce 64 bits of cipher text. The same algorithm and key are used for encryption and decryption. DES has a key length of 56 bits, since 8 of the 64 bits of the key are not used by encryption algorithm. The two properties make cipher very strong that is avalanche effect and completeness. The discomfort in speed of exhaustive key searches led to introduce triple DES. Triple DES systems design is an encrypt- decrypt – encrypt process. It provides backwards compatibility with DES. Triple DES is more secure than single DES but slower process then encryption using single DES.

1.4 RSA ALGORITHM

RSA is an asymmetric encryption/decryption algorithm. Encryption of the message can be done using the public key that is distributed to all and the decryption can be done using the private key which is kept secret. In cloud computing, the data security can be achieved by RSA algorithm. When the data is encrypted and stored in the server only authenticated users can able to decrypt the data from server.

1.5 SECRET SHARING

The secret can be recovered from certain pieces of information are called sharing protocols or secret sharing. It is based on polynomial evaluation. Shadows are derived from secret but not part of secret. Different values obtained from secret but these values don't give clue about content of the secret. Shadows are same size of secret called ideal protocol. If n shadows are generated we need k of them to recover. K is the threshold value which is known as threshold protocol. If the shadow less than K, it cannot able to recover.

Suppose our secret is JK. Divide the secret in to 6 parts (n=6) , where any subset of 3 parts (k=3) is sufficient to reconstruct the secret. At random get 2 numbers N1 and N2.

The polynomial is $f(x) = JK + N1x + N2 x^2$.

6 points are constructed from the polynomial: (X0,Y0) (X1,Y1) (X2,Y2) (X3,Y3) (X4,Y4) (X5,Y5).

Any 3 points are enough to reconstruct the secret. Consider 3 parts.

$$(x_0, y_0); (x_1, y_1) ; (x_2, y_2)$$

By Lagrange interpolation method,

$$l_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} \quad l_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} \quad l_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1}$$

Therefore:

$$f(x) = \sum_{j=0}^2 y_j \cdot l_j(x)$$

Thus original polynomial is obtained.

1.6 BEE'S LIFE ALGORITHM

Bee's life algorithm is a search method inspired from the behaviour of honey bees. The algorithm used to find solution for optimisation problem. Bees are the agents who search the solution space and each time a bee visits flower it evaluates its profitability. Algorithm consists of initialisation and a main search cycle. Each search cycle contains five steps such as recruitment, steps such as recruitment, local search, neighbourhood shrinking, site abandonment, global search. First initialise population with random solutions. Evaluate the fitness of the population. From new population if stopping criteria is not met. Select the sites for neighbourhood search and recruit bees for selected sites. Evaluate fitness and select the fittest bee from each patch finally assign remaining bees to search randomly and evaluate their fitness. The honey bee foraging algorithm can be used in cloud computing for load balancing servers are bees and web applications are flower patches. An advert board is used to simulate waggle dance. Each server is either a forager or a scout. The advert board is where servers success fully fulfilling a request or may place adverts.

2. LITERATURE SURVEY

Tanjyot Aurora et al (2013) [2] The paper proposes a design and implementation of blowfish algorithm for the confidentiality of private information.it is a symmetric block cipher designed by Bruce Schneier which is fastest one. Blowfish has 16 rounds. Each one consists of key dependent permutation. The algorithm can be effectively used for encryption and safeguarding data. It is suitable for application like a communication link or an automatic file encryption.

Kadwe Yugandhara et al (2016) [1] The paper proposes a secured cloud storage system for data forwarding and data storage. The encrypted data are partitioned and store in storage server. The data stored in the server will be secured during transmission. The datas are protected from hackers and intruders.it helps the user to send data without hesitation of data being lost.

Saikumar Manku et al (2015) [3] The paper analyse the blowfish encryption algorithm. The algorithm reduces rounds of algorithm and proposed single blowfish round. VHDL language is used for design simulation. The 64 bits are separate in to 32 bits and there will be four s-boxes and each contains 32bits. The two s-boxes connecting with XOR then from the two XOR added then w get the plain text.

Manisha Mankar et al (2015) [3] Rijndael is one of the efficient cryptographic technique that have iterative looping approach. The paper proposes 192 bit key size cipher. Rijndael algorithm is introduced to replace DES algorithm. It can use key length of 128,192,256 bits. The algorithm composes of three main steps, cipher, inverse cipher and key expansion. Cipher converts the data back to plain text. Key expansion generates a key schedule that can be used in the encryption and decryption. Number of rounds is based on the key length.

Tasquia Mizan et al (2012) [4] In cloud computing job scheduling problem can be solved using Bees Life algorithm. It is a greedy method for hybrid cloud. The paper proposes how to minimize the makespan which is a major issue in job scheduling. The algorithm enhances the efficiency of scheduling in cloud. The algorithm has less makespan than firefly algorithm or genetic algorithm. The efficiency of cloud computing services relate to the performance of cloud job scheduler in the cloud

data center. When multiple cloud users request for data center access, a non-primitive priority queue is used. Grid Information System is responsible to allocate the tasks. Bees Life algorithm will randomly select set of tasks for one data center and find nearest idle data center and resource in the cloud to reduce the makespan.

3. CONCLUSION

The demand of cloud is increasing day by day. Emphasis must be given to secured data forwarding over cloud, resource allocation in cloud. Encryption algorithm plays important role in data security on cloud. To reduce the network traffic among resources in cloud role of load balancing algorithm is crucial. By comparing different parameters used in algorithm, AES is found to be faster compared to others in terms of execution time. DES algorithm consumes least encryption time but its execution time is longer. RSA consumes longest encryption time and memory size. it is not scalable. Secret sharing protocol provides high security for the data. it is used in military device initialization. Blowfish has least memory requirement. Blowfish is suitable for applications like communication link encryption where the key remains constant for a long time.

ACKNOWLEDGEMENT

The authors would like to thank Mr. Jayakrishnan. k. Also we would like to thank the reviewers for the improvement of my paper.




REFERENCES

- [1] Jadhav Ashwini, J. S. Pawar, Kadwe Yugandhara, Pagar Pooja, Patil Suchita, "Secure Data Storage and Forwarding in Cloud using AES and HMAC", International Research Journal of Engineering and Technology, February 2016.
- [2] Parul Arora, Tanjyot Aurora, "Blowfish Algorithm", International Journal Of Computer Science and Communication Engineering, 2013.
- [3] K. Vasanth, Saikumar Manku, "Blowfish encryption algorithm for information security", ARPN journal of engineering and applied sciences, June 2015.
- [4] Rohaya Latip, Shah Murtaza Rashid Al Masud, Tasquia Mizan, "Modified bees life algorithm for job scheduling in hybrid cloud", International journal of engineering and technology, July 2012.
- [5] Randeep Kaur, Supriya Kinger, "Analysis of security algorithm in cloud computing", International journal of application or innovation in engineering and management, March 2014.
- [6] Rachna Arora, Anshu Parashar, "Secure user data in cloud computing using encryption algorithms", International journal of engineering research and algorithms, August 2013.
- [7] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z, and Song D, "Provable Data Possession at Untrusted Stores", Proc. 14th ACM Conf. Computer and Comm. Security (CCS), pp. 598-609, 2007.
- [8] Ateniese G, Benson K, and Hohenberger S, "Key-Private Proxy Re-Encryption", Proc. Topics in Cryptology (CT-RSA), pp. 279-294, 2009.
- [9] Ateniese G, Fu K, Green M, and Hohenberger S, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", ACM Trans. Information and System Security, vol. 9, no. 1, pp. 1-30, 2006.

[10] Ateniese G, Mancini L.V ,Pietro R,D and Tsudik G, “Scalable and Efficient Provable Data Possession,”Proc. Fourth Int’l Conf. Security and Privacy in Comm. Netowrks (SecureComm),pp 1-10, 2008.

[11] Blaze M, Bleumer G, and Strauss M, “Divertible Protocols and Atomic Proxy Cryptography,”Proc. Int’l Conf. Theory and Applica-tion of Cryptographic Techniques (EUROCRYPT),pp 127-144, 1998.

ABOUT AUTHORS

	<p style="text-align: center;">ROSHITHA P P</p> <p>Pursuing M.E(Computer Science and Engineering) in Maharaja Institute of Technology. Have keen interest in the Cloud Computing, Networking and Mobile Computing.</p>
	<p style="text-align: center;">NOWSHAD M U</p> <p>Pursuing M.Tech in Royal College of Engineering and Technology. Have keen interest in the machine learning, artificial intelligence and Robotics. Done projects in the Image processing and Speech and Language processing. 3 years of Industrial experience in India and GCC.</p>
	<p style="text-align: center;">T SIVAKUMAR</p> <p>Head of the Department and Assistant Professor in Maharaja Institute of Technology. Have keen interest in the Data Mining. Done projects in Data Mining, Data Source and Data Warehousing. 10 years of Teaching experience in India.</p>