International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 7, Issue 1, January - February 2018 ISSN 2278-6856

Application of co-operative encryption to Clouds for Data Security

Dr. V. Nandakumar[1]

[1]Senior Programmer, Computer Centre, Alapappa University, karaikudi, Tamilnadu, India

Abstract

Cloud computing originated for daily Computing Problems and needs. It is an internet paradigm developed with computer technology as the base. It offers an effective pool of resources using the internet medium. Every paradigm has its own set of challenges and problems. This paper analyses the problems of data security and access anonymity in cloud computing. The paper proposes a new technique for data security in cloud computing called Secure Cloud Data with servers using Encryptions. The paper further attempts to eliminate concerns on data privacy using encryption algorithms and thus enhancing security in a cloud infrastructure.

Keywords: Cloud Computing, Encryption, Cloud Security, Co-operative keys

1. INTRODUCTION

Cloud computing offers services to customers over a network with the ability to dynamically change or service requirements. It allocates storage and computing resources on demand or actually shares resources to customers [1] [2]. The cloud infrastructure and services are generally offered by third party vendors for public use who offer cloud services based on their network and computing infrastructures [3 - 13]. Though these virtual services make an effort to be reliable, security in the cloud can be a major impediment when dealing with public domains. Data security then becomes an important parameter of quality assurance. Imposed security is required while accessing data. Cloud systems are powerful than personal computers, but have external and threats as an unwanted obstacle. Cloud Computing reduces hardware costs provided to users on demand on pay per use basis and in three forms Software as a Service (SAAS) or Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). SaaS is the set of applications offering anywhere access on a cloud, but comes with increased security risks. PaaS shares the development environment allowing user control applications to be deployed. Security of cloud based data is a shared responsibility between service providers and users. Thus data encryption can play a major role while accessing sensitive data. Fernandes, D., et al.. in their study stress on security requirements imposed by cloud service models [14].

2. SECURITY CHALLENGES IN CLOUD COMPUTING

In any cloud deployment, storage, platform, software and networking are a part of the cloud infrastructure. Clouds are deployed as private or public or hybrid models. Private clouds are within an organization like an internal data center[15]. Private clouds attempt to address concerns on data security with greater control. Public clouds, generally owned by third parties are like an organization having an offline data centre. They are a pay-per-use cloud catering to the demands of users and are optimized [16]. Since, Public clouds use internet medium they are less secure. Hybrid cloud is a mix of the other two models where a part of the cloud public. Hybrid clouds are managed centrally, making it a single logical unit with a secure network [17]. Across these models security is a critical aspect of cloud computing as the data stored on the cloud is important and sensitive [18]. The infrastructures used in cloud computing have not been evaluated completely on security. There are many concerns like trust, security and performances in securing a cloud. Security concerns on the cloud are a combination of provider security and breaches in user security [19]. Management of user identity and authentication can help improve security on the cloud [20]. Another issue in clouds is the risk of malicious players causing failure of cloud services. Confidence in cloud infrastructure is attained when users are assured that their data will be confidential in the cloud [21]. In access control, moderate access control leads to unauthorized access, thus decreasing security in access [22][23]:

3 SECURITY ALGORITHMS IN CLOUD COMPUTING

3.1 RSA

RSA is a popular Public-Key algorithm widely used to provide security to data. It stands for Ron Rivest, Ada Shamir and Len Adleman, who first proposed in 1977. Data is encrypted to provide security and the targeted user can access the data based on an encryption key. On a data request from the user, the request is forwarded to the cloud provider. The cloud application then authenticates the user's authenticity before data is provided to the user. RSA uses a public key and a user's private key to encrypt or decrypt the data. RSA thus consists of a Key Generation , Encryption and Decryption. The disadvantages of RSA are that it can encrypt only small amount of data. Figure 1 depicts a secure cloud architecture.

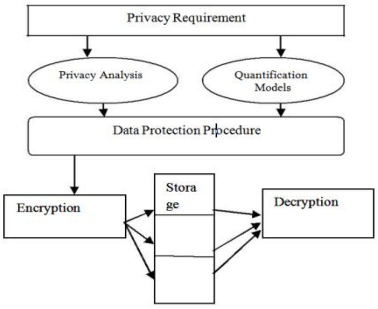

Figure 1 Secure Cloud Architecture [24]

3.2 AES

AES is based on the Rijndael cipher[25] developed by Joan Daemen and Vincent Rijmen and submitted to NIST [26] .Rijndael is a family of ciphers with different key and block sizes.AES-128 used at client level for data encryption before data is transmitted to the cloud application provider. Then, since application uses SSL as well and an additional point of encryption is applied during data transmission. The data is stored as encrypted on the company servers, along with the public key that is in turn encrypted with a hash of the users password. As AES is used widely now-a-days for security of cloud. Implementation proposal states that First, User decides to use cloud services and will migrate his data on cloud. Then User submits his services requirements with Cloud Service Provider (CSP) and chooses best specified services offered by provider. When migration of data to the chosen CSP happens and in future whenever an application uploads any data on cloud, the data will first encrypted using AES algorithm and then sent to provider. Once encrypted, data is uploaded on the cloud, any request to read the data will occur after it is decrypted on the users end and then plain text data can be read by user. The plain text data is never written anywhere on cloud. This can be integrated without any changes to application. The key is never stored next to the encrypted data, since it may compromise the key also. To store the keys, a physical key management server can be installed in the user‘s premises. This encryption protects data and keys and guarantees that they remain under user‘s control and will never be exposed in storage or in transit. AES has replaced the DES as approved standard for a wide range of applications.

3.3 DES

The Data Encryption Standard (DES) is a block cipher, which encrypts 64 bit data to produce 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences. The key length of this algorithm is 56 bits; however a 64 bits key is actually input. DES is therefore a symmetric key algorithm. The strength of DES lies on two facts: The use of 56-bit keys: 56-bit key is used in encryption, there are 256 possible keys. A brute force attack on these keys is not feasible. The nature of algorithm: Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.

3.4 Co-operative Keys

Most attacks on cryptosystem are focused on the implementations and protocols that use the algorithm. Attackers look for small flaws or cracks that they can exploit in a system to gain access. Text files after encryption remain as temporary files or virtual memory. Old keys left on the hard disk to recover data in cases of emergencies and copies of text files are exploited by attackers. Sharing or reusing passwords are all ways to corrupt the integrity of a system. Cracking a code involves either an attack on code itself or on way it is used. The real risk lies in how the cipher codes are actually used. Stronger subsystems present a larger work factor while weaker systems are easier to overcome. Dr. Nandakumar proposed a Co-operative Key Encryption in [27] and depicted in Figure 2. It is a block cipher with the powerful influence on cryptography, where both the sender and receiver agree on two numbers “p” and “g”, where p is a large prime number and g the base generator. Sender then chooses his secret even number called “a”. Similarly the Receiver’s secret even number is “b”. Sender and Receiver exchange their numbers. Sender knows p, g, a, b and the Receiver knows p, g, b, a. The sender Computes the Key for Encryption as $K1_a = g^a$ mod p and $K2_a = g^b$ mod p. The key is generated in 128 bits as its key length. $K1_a$ forms the first part of the Symmetric key. $K2_b$ second part of the encryption key as demonstrated in Figure 5.1 where Key $K = k1_a \| k2_b$. The Key is then used to encrypt the data blocks of 128 bytes and sent. The receiver Computes the Key for Decryption as $K1_a = g^a$ mod p and $K2_b = g^b$ mod p. The sender is the cloud infrastructure service provider while the receiver is the user.

64 bit key of Cloud Provider	64 bit key of Cloud user

Figure 2 128 bit co-operative Encryption Key

3.4.1 Encryption and Decryption

The file to be encrypted of length m is split into message blocks of size 128. Each Message bit M is clubbed with the corresponding key bit K in an exclusive OR operation to form the Cipher text. The resultant Cipher text is rotated left a sum b times in single digit where a is the Sender’s secret even number and Receiver’s secret even number is b, to generate the final output of the Cipher text block. During Decryption,, the encrypted file is split into message blocks of 128 bits and each ciphered block is rotated right a sum b times in single digit where a is the Sender’s secret even number and Receiver’s secret even number is b. The resultant Cipher text bit is clubbed with the corresponding key bit K[i] in an exclusive OR operation to retrieve the original Message and eventually the file. The cop-operative key technique is advantageous, since the key length of 128 is large, it is difficult to trace this key in exhaustive key searches. It is also secure against known cryptanalytic techniques like differential and linear cryptanalysis. Though the key can be broken into two 64bit keys and seems insecure against linear or differential cryptanalysis, these attacks are impractical. The effective key length of 128 bits is large enough for security.

3.4.2 Comparative Results of co-operative keys

The time delays for encrypting/decrypting of 1Kilobit of data of co-operative key and other crypto keys are shown in Table 1.

Table 1: Encryption/Decryption Time [27]

Algorithm	Time in Sec/Kilobit	
Key Size	Encryption	Decryption
DES 56 bit	0.285714286	0.222258286
3DES 56 bit	0.857142857	0.793686857
AES 128 bit	0.246796875	0.246896875
Blow Fish 128 bit	0.208828125	0.008158124
CKE 128 bit	0.07846875	0.070621875

The above table obviously shows that the time taken for encryption and decryption of AES and co-operative keys equal. Similarly, the time taken for encryption and decryption of co-operative is also equal. But other methods have some differences of time in performing encryption and decryption process. Co-operative keys reduce time taken for encryption and decryption than other methods. Again the 3DES on 56 bit shows higher time over other methods. And the time for DES and 3DES may be higher if higher keys involved in process. The study in [27] also found that the encryption and decryption time of co-operative keys on various flat file was the same.

3.4.3 Security Analysis

The security level is defined by the strength of keys, the mathematical logic used to mix key bits with data bits to generate cipher text and amount of time taken to break the key. In co-operative keys, numbers necessary for generating the symmetric key are communicated rather than the symmetric keys. To confuse attacks, the key elements are shifted left one time and added together till it gives single digit. This digit is sent to the respondent with the key generating elements for maximum security. Since co-operative keys is a combination of sender and receiver part of keys, the sender alone cannot encrypt a message without the knowledge of the receiver. The security of keys is determined by the key size of their outputs, n. The method discussed in this paper has the same attack complexity, but the permutation process increases the attack complexity in proportion to the size of the secret key. Since a 128-bit secret key is used, permutation complexity becomes which yields the total complexity of $2!2^{7}! \times 2^{128}$ and is secure. The attacker picks some pair (l, r) from S and outputs Tl || Tr, thus returning a key consistent with the input-output example (M1,C1). The set S above is likely to be quite large, of size about $2^{64+64}/2^{64} = 2^{64}$, means the attack is not likely to return the target key. Trying a few more input-output examples, it is easy to jot down the choices in the set S until it is likely that only the target key remains. The attack makes $2^{64} + 2^{64} = 2^{65}$ co-operative keys or co-operative keys^{-1} computations. The step of forming the set S can be implemented in linear time in the size of the arrays involved. Thus the running time is dominated by the co-operative keys, co-operative keys^{-1} computations. The meet-in-the-middle attack shows that co-operative keys are quite far from a cipher where the best attack is exhaustive key search. Hence this attack is impractical, even with the best of the machines. The machines can do the computations quickly, but to form the set the attack needs to store the arrays L,R, each of which has 128 entries, each entry being 128 bits.

The amount of storage required is $16 \cdot 2^{128} \approx$ results in terabytes, which is so large, that implementing the attack is impractical. There are some strategies that modify the attack to reduce the storage overhead at the cost of some added time, but still the attack does not appear to be practical. Since a 128-bit co-operative keys key can be found using 2^{128} co-operative keys or co-operative keys^{-1} computations, implies co-operative keys has an effective key length of 128. Let E: K × {0, 1}n → {0, 1}n be a block cipher. Operating it in co-operative keys yields a stateful symmetric encryption scheme, SE = (K, E,D). The key generation algorithm returns a 128 bit key for the block cipher. The encryption procedure can be executed in parallel for speeding up the processes in the presence of hardware support. The methods work for strings of arbitrary bit lengths. Table 2 list a comparison between encryption algorithms with respect to security

Table 2: comparison between encryption algorithms with respect to security [27]

Characteristics	RSA	AES	DES	Blowfish	co-operative keys
Key Size	1024 bits	128 bits	56 bits	32-448 bits	128 bits
Keys Used	Public key for encryption & private key for decryption	Same key for encryption & decryption	Same key for encryption & decryption	Same key for encryption & decryption	Same key for encryption & decryption
Security	Secure for user only	Secure for user and provider	Secure for user and provider	Secure for user and provider	Secure for user and provider

4 CONCLUSION

This paper has analyzed different methods for data security in cloud using encryption algorithms. The paper has detailed on security challenges in the cloud while detailing a comparison of encryption algorithm in the cloud. Encryption algorithms can play a major role in cloud data security. The paper has also proposed the technique of co-operative usage in the cloud for security.

References

[1] Panagiotakis, S., Vakintis, I., Andrioti, H., Stamoulias, A., Kapetanakis, K., & Malamos, A. (2015). Towards Ubiquitous and Adaptive Web-Based Multimedia Communications via the Cloud. In G. Mastorakis, C. Mavromoustakis, & E. Pallis (Eds.) Resource Management of Mobile Cloud Computing Networks and Environments (pp. 307-360). Hershey, PA: Information Science J. Moura, and D. Hutchison Reference. doi:10.4018/978-1-4666-8225-2.ch011

[2] Fernando, Niroshinie, Seng W. Loke, and Wenny Rahayu. 2013. Mobile Cloud Computing: A Survey. Future Generation Computer Systems (Elsevier Science Publishers B. V.) 29, n.º 1 (#jan# 2013): 84-106.

[3] AT&T. AT&T Cloud Architect. 2012. http://cloudarchitect.att.com/Home/ (retrieved 02/03/2014). Aazam, M., Huh, E.-N., Kim, S.. 2015. Inter-Cloud Computing Architecture, IETF Informational document, draft-aazam-cdni-inter-cloud-architecture-02 (Expires in 17/09/2015), 22 pages

[4] BT. Cloud Compute. 2014. http://www.globalservices.bt.com/uk/en/products/cloud_compute (retrieved 02/03/2014).]

[5] DT. Cloud. 2014. http://www.telekom.com/innovation/80328 (retrieved 02/03/2014).

[6] MT. SAAS Application Hosting. 2014. http://www.macquarietelecom.com/solutions/pure saas-application-hosting/ (retrieved 02/03/2014).

[7] ND. Cloud Solutions. 2014. http://www.nttdata.com/global/en/services/cloud/index .html (retrieved 02/03/2014).

[8] PT. Cloud Solutions.2014. https://cloud.ptempresas.pt/Pages/Catalog/ ServiceDetail.aspx?s= 06IG3nFf0pSkKNHn-KBVCw&language=en-US (retrieved 02/03/2014).

[9] Amazon. Elastic Compute Cloud. 2013. https://aws.amazon.com/pt/ec2/ (retrieved 02/03/2014).

[10] Dropbox. Dropbox. 2014. https://www.dropbox.com/ (retrieved 02/03/2014).

[11] Google_a. Google App Engine: Platform as a Service. 07/02/2014. https://developers.google.com/appengine/ (retrieved 02/03/2014).

[12] Microsoft_a. Windows Azure. 2014. https://www.windowsazure.com/en-us/ (retrieved 02/03/2014).

[13] Salesforce. Salesforce1 Platform. 2014. http://www.salesforce.com/eu/platform/overview/ (retrieved 02/03/2014).

[14] Fernandes, D., et al.. 2014. Security issues in cloud environments: a survey. Int. J. Inform. Sec. 13 (2), 113–170.This paper proposes a secure and robus encryption model for cloud security.

[15] S.Arnold.2009.Cloud computing and issues of privacy

[16] A Platform Computing Whitepaper. Enterprise Cloud Computing: Transforming IT. Platform Computing, pp6, 2010.

[17] Global Netoptex Incorporated. Demystifying the cloud. Important opportunities, crucial choices., pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[18] Nisha Yadav and Dr. Amit Sharma "IMPLEMENTATION OF DATA SECURITY IN CLOUD COMPUTING", Internation journal of advanced technology in engineering and science, vol. no. 4, issue no.4, April2016

[19] SUDARSHAN ADEPPA, SECURITY ANALYSIS IN CLOUD COMPUTING ENVIRONMENT, Proceeding of NCRIET-2015 & Indian J.Sci.Res. 12(1):381-384, 2015 ISSN: 0976-2876 (Print) ISSN: 2250-0138

[20] 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 4(19): 3574-3579, 2012 ISSN: 2040-7467

[21] Parsi Kalpana,Sudha Singaraju. 2012 Data Security in Cloud Computing using RSA Algorithm. International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4.

[22] ZiyuanWang .2011.Security and privacy issues within the Cloud Computing‖ , International Conference on Computational and Information Sciences.

[23] K.Sravani, , K.L.A.Nivedita .Effective Service Security Schemes In Cloud Computing".International Journal Of Computational Engineering Research (ijceronline.com) Vol. 3 Issue. 3

[24] I-Hsun Chuang,Syuan-Hao Li,Kuan-Chieh Huang,Yau-Hwang Kuo. 2011. Effective privacy protection scheme in cloud computing. ICACT

[25] Rachna Arora, Anshu Parashar. 2013. Secure User Data in Cloud Computing Using Encryption Algorithms (IJERA) Vol. 3, Issue 4

[26] Mandeep Kaur, Manish Mahajan. 2013. Using encryption Algorithms to enhance the Data Security in Cloud Computing. International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03.

[27] Dr. V.Nandakumar, A New Co-Operative Key Generation Technique for Symmetric Encryption, (IJITR) International Journal Of Innovative Technology And Research, Volume No. 1, Issue No. 4, June - July 2013, 292 - 294., ISSN 2320 –5547 @ 2013

AUTHOR

Dr. V. Nandakumar is presently working as Senior Programmer in Computer Centre, School of Computational Sciences, Alagappa University since 1986. He received Doctoral Degree in 2011 from Alagappa University. He has published about 15 publications National and International level.