Journal of Engineering and Applied Sciences 13 (8): 2057-2061, 2018
ISSN: 1816-949X

Enhancement of Digital Signature Using Hybrid Key Generation Scheme in Cloud

[1]Sumit Chaudhary, [2]Neeraj Kumar Pandey and [3]Narendra Kumar Joshi
[1]Department of IIST, Cadila Group, Kadi, Ahmedabad, Gujarat, India
[2]GLA University, Mathura, Uttarpradesh, India
[3]Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, Uttarakhand, India

Abstract: Cloud data outsourcing is all about services over the internet when we access the services, security is a major concern. The main aspect in the use of any cloud services is data security, confidentiality and integrity. Cloud computing provides a virtual environment to the user to access computing power or resources (e.g., Storage, application, server, services and network) that exceed what we have within our physical world. Once the user uses the virtual cloud environment after that cloud user must transfer any data through the cloud. As far as security is a concern, data encryption is one way to protect our data before outsourcing. With the combination of a convenient asymmetric and symmetric encryption scheme, strategy is developed. Using hybrid key generation scheme data transfer can be done and secure encryption is achieved. For the decryption algorithm the user's public key is required and applied in digital signature algorithm. As soon as recovery of symmetric key is complete, it is ready to use for decrypting the message. Various benefits can be provided by using combination of encryption methods. Connection can be establish between among two users with the improved encryption technique and that will be more secured. Communication can be done between users with this hybrid key Algorithm. The encryption process can be slow down using symmetric encryption but simultaneously using asymmetric encryption, both forms of encryption can be enhanced. Thus in the data encryption or decryption, key management is also the challenging issue.

Key words: Cloud computing, hybrid key generation, key management, data security, digital signature, decryption

INTRODUCTION

Cloud computing (Nagamalli *et al*., 2014; Blundo *et al*., 2009; Thiyagarajan and Ganesan, 2015; Chehal and Singh, 2012; Kalpana and Singaraju, 2012) always has the challenge of security as security is difficult to implement in the cloud. This study is all about security challenges which are faced when the storage is done in the cloud. Basically, the vendors provide cloud storage to its customers without following any security methods. Data safety is not that much ensures by any cloud provider and the integrity of data is not sure. In this, a hybrid encryption technique is used for the data security. A type of encryption (Zhou *et al*., 2011; Grace and Sumalatha, 2014; Wang *et al*., 2010) that merges two or more form of encryption is known as hybrid encryption. This hybrid encryption will have advantages from both asymmetric as well as symmetric encryption (Zhou *et al*., 2011; Grace and Sumalatha, 2014; Wang *et al*., 2010). Through this technique we can increase the strength of encryption algorithm and also decryption algorithm. The two characteristics which act as major strengths are speed and security. The hybrid encryption is strongly secure encryption as it has major security features, i.e., combination of public and private keys. With the combination of a convenient asymmetric encryption scheme is developed. Using various unique keys data transfer can be done and hybrid encryption (Hatzopoulos *et al*., 2013; Hu *et al*., 2011; Takouna *et al*., 2014; Zhou *et al*., 2011; Yu *et al*., 2010) is achieved. Also for random symmetric key encryption (Saini and Sharma, 2014; Moorthy and Sivasubramaniam, 2012; Kaur and Kaur, 2015; Prasad *et al*., 2011; Liu *et al*., 2012; Shah *et al*., 2015; Sharma and Banga, 2013) public key encryption can be used. If decryption of symmetric key has to be done then the recipient can use the public key encryption technique. The message encryption done by applying the recovery of the symmetric key.

The combining and mixing of various encryption techniques has its own benefits and advantages. One basic benefit of combination is there can be connection between two or more users and the equipment. With the

Corresponding Author: Sumit Chaudhary, Department of IIST, Cadila Group, Kadi, Ahmedabad, Gujarat, India

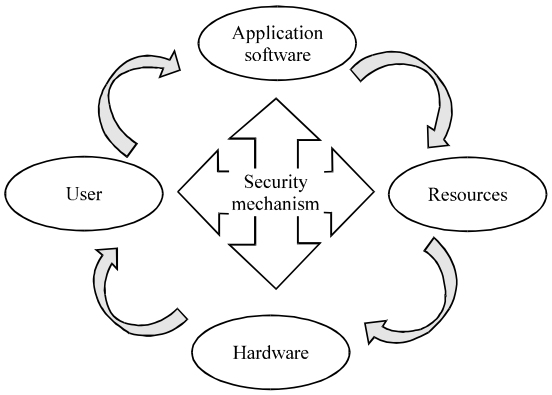

Fig. 1: Integration of data security

help of this hybrid encryption method communication or link can be made between the users. If we use asymmetric encryption technique the encryption process can be slow down but on the other hand if we use symmetric encryption then encryption of both forms can be enhanced simultaneously. The overall system performance can be improved with the result of added security in the transmittal process. The hybrid cryptosystem (Hatzopoulos *et al*., 2013; Hu *et al*., 2011; Takouna *et al*., 2014; Zhou *et al*., 2011; Yu *et al*., 2010) is a public key system whereas same as the key encryption scheme its public as well as private keys, i.e., both keys are the same. A digital signature can also be used as function with message digesting features having a symmetric key system in place of a key system which uses a public key in the making of a hybrid cryptographic system. The message can be long or short like if our message is very long then we require some more efficient symmetric key for the encryption as well as decryption whereas if our message is short then the use of some type of public key can be used. For example, for encrypting any message that is addressed to some user-1 in some hybrid method user-2 can have the following (Ezzarii *et al*., 2015) (Fig. 1).

Literature review: Various encryption algorithms hide a sequence of bits into random number generator function from other plain text message. It is an encryption algorithm which can be used for secure data over communication. As the name suggests its basic functions, which include insertion and hiding of plain text and the term hybrid is used as it has features of data hiding techniques. Ramaraj *et al*. proposed a encryption technique using hybrid method for security of online transaction. The combination of symmetric as well as asymmetric cryptographic methods is known as the hybrid encryption technique. This hybrid method provides all the main three cryptographic security properties these are, integrity, confidentiality and authentication. With the combination of symmetric cipher and public key which is RSA with some hash function a new design protocol is proposed. Encryption can be converted in some form that will make it difficult to read and make it more secure. In this method some substitution is done with each letter of plaintext replaced by fixed count of alphabets. As Julius Caesar used this method for communication with his generals, so, it was named after him. The final result can be a data which now decrypted again from its encryption form. So, we can say that Caesar cipher algorithm can be used to secure data using hybrid encryption techniques. Kuppuswamy and Chandrasekar's describes one new algorithm which deals with linear block cipher. This concept is completely based on modular 37 which means alphabets and numerals both can be used. Whereas previous algorithms based on only modular 26 (only alphabets).

Kuppuswamy and Al-Khalidi proposed that providing security in the network with the help of better encryption techniques by implementing them in simple and powerful method should be the research main goal. This study proposed a technique using modular 37 which selects any number randomly and after that its inverse is calculated by using some modular 37 technique and we should done that distribution of the symmetric key in a very secured way. We have to also calculate the effectiveness of the new algorithm by comparing it with other symmetric algorithm which already exists.

Sood (2012) proposed that in information technology which has some major features like performance, accessibility, low cost etc used in cloud. Using this method we can increase the new capabilities by not investing much in stuffs like infrastructure, having new personnel and buying or licensing some new software from the market. This helps in providing huge amount of data storage and fast processing for its customers over the network. As it can send large data or database and its applications to the centers known as cloud. Large companies want to deploy cloud in their business as it provides huge variety of luxuries. Security of data can be the major challenge in the area of cloud that works as a challenge while implementing cloud. In this study we have proposed a frame work which comprises of different techniques with different methods or procedures and all these help in securing our database at all the stages, starting from its master to cloud's end user.

MATERIALS AND METHODS

Proposed system: Algorithm of hybrid key generation process at sender side.

Phase 1; Private key (k1) generation RSA:
Step 1: select two prime number a, b
Step 2: calculate x = a*b

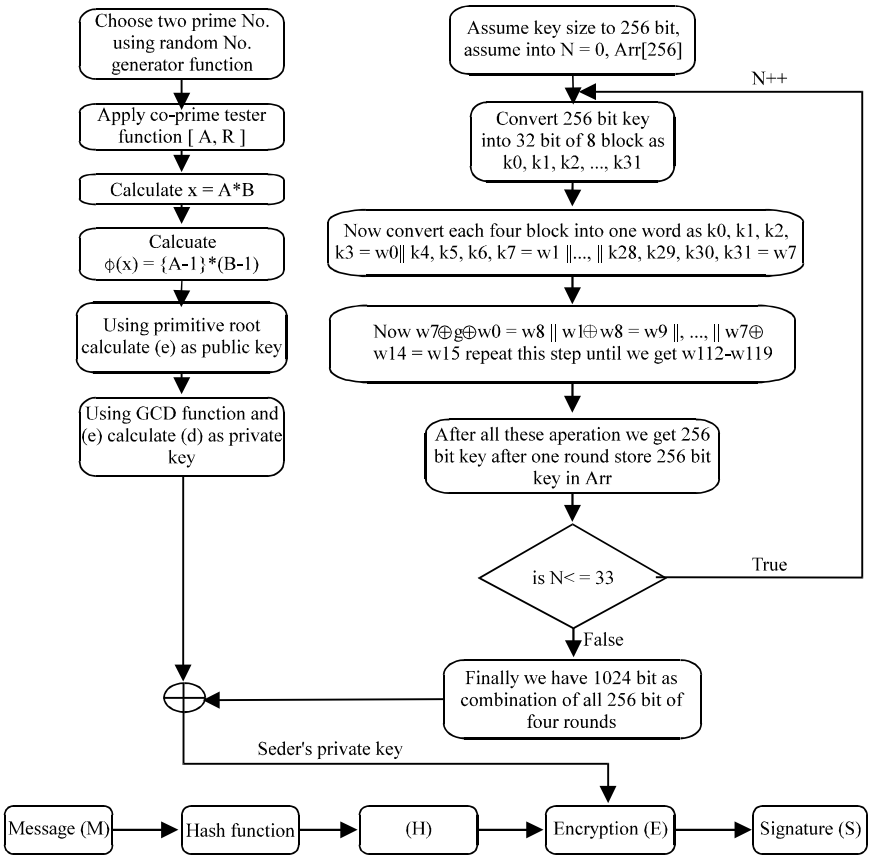

Fig. 2: Sender side encryption algorithm using hybrid key generation

Step 3: Calculate ø (x) = (a-1)*(b-1)
Step 4: select public key e: gcd (e, ø (x)) = 1 Step 5: determine 1024 bits private key y: ye = 1 (mod ø(x)) where y<ø(x)
Step 6: Select random 256 bits key k1
Step 7: calculate KeyExpansion() Function
Step 8: repeat step 6 with keys k2 , k3, k4
Step 9: determine 1024 bits z : k1+k2+k3+k4
Step 10: calculate final 1024 bits key k: y×z
Step 1: apply final key k as private key in digital signature algorithm for encryption

Phase 2; Private key (K2) generation using Modified AES (MAES) algorithm:

Code of Keyexpansion function
KeyExpansion(byte key (Xiao and Xiao, 2013), word)
{
word x;
for (a = 0; a<8; a++)
{
w[a] (key[8*a], key[8*a+1], key[8*a+2], key[8*a+3], key[8*a+4], key[8*a+5], key[8*a+6], key[8*a+7])
for (a = 8; a<112; a++)
{
x = w[a-1]
if(A mod 8 = 0)
x = SubWord (RW (x))/Rcon[a/8]
w[a] = w[a-8]/x
}
}
g function process

Step 1.RW performs one-byte circular left shifts on a word .ex input word [A0, A1, A2, A3, A4, A5, A6, A7] is transformed into [A1, A2, A3, A4, A5, A6, A7, A0].
Step 2. Using S-box, Sub Word byte substitution on each byte of its input word is performed.
Step 3. After that step 1 and step 2 results is XORed with a round constant, Rcon [j]

Phase 3; Digital signature algo using HKG (hybrid key generation) as H_k(K1, k2):

Step 1. $E(PR_{(k1?K2)},H(M))\_ S$
Where H(M) is Hash function of Message
K1 is Private Key Generation using RSA
K2 is Private Key Generation using MAES
S is digital Signature
H_k (K1, K2) is Hybrid Key Generation
Algorithm of hybrid key generation process at receiver side.
Step 1. $D(PU_s , S) \_H_s(M)$
Where S is digital Signature
Step 2. Determine H(M) by applying Hash Function on message
Step 3. Compare $H_s(M)$ and H(M) (Fig. 2)

CONCLUSION

This study propose a better data security scheme with the help of a hybrid encryption algorithm with the combination of using RSA and AES algorithms in the

cloud. The main and foremost advantage of this algorithm is that it provides key generation on the basis of time of system so making it more secure as no intruder can guess. User only knows the private and secret key, so, security increased itself with convenience and even cloud administrator cannot access. The reason behind using the combination of both the RSA and AES encryption that it is providing us some encryption with public key and then decryption by using private and secret key. The data then uploaded on cloud using encryption and then can be decrypted with the help of a private key and the secret key of the user.

REFERENCES

Blundo, C., C. Stelvio, C.D.V. De, Sabrina, A. De Santis and S. Foresti *et al*., 2009. Efficient Key Management for Enforcing Access Control in Outsourced Scenarios. In: Emerging Challenges for Security, Privacy and Trust, IFIP Advances in Information and Communication Technology. Gritzalis, D. and J. Lopez (Eds.). Springer, Boston, Massachusetts, ISBN:978-3-642-01243-3, pp: 364-375.

Chehal, R., K. Singh and K. Singh, 2012. Efficiency and security of data with symmetric encryption algorithms. Intl. J. Adv. Res. Comput. Sci. Software Eng., 2: 472-475.

Ezzarii, M., H. El Ghazi, H. Elghazi and T. Sadiki, 2015. Performance analysis of a two stage security approach in cloud computing. Proceedings of the 2015 International Conference on Cloud Technologies and Applications (CloudTech'15), June 2-4, 2015, IEEE, Marrakech, Morocco, ISBN:978-1-4673-8150-5, pp: 1-7.

Grace, S.S. and M.R. Sumalatha, 2014. SCA-An energy efficient transmission in sensor cloud. Proceedings of the 2014 International Conference on Recent Trends in Information Technology (ICRTIT'14), April 10-12, 2014, IEEE, Chennai, India, ISBN:978-1-4799-7868-7, pp: 1-5.

Hatzopoulos, D., I. Koutsopoulos, G. Koutitas and W.V. Heddeghem, 2013. Dynamic virtual machine allocation in cloud server facility systems with renewable energy sources. Proceedings of the 2013 IEEE International Conference on Communications (ICC'13), June 9-13, 2013, IEEE, Budapest, Hungary, ISBN:978-1-4673-3122-7, pp: 4217-4221.

Hu, H., J. Xu, C. Ren and B. Choi, 2011. Processing private queries over untrusted data cloud through privacy homomorphism. Proceedings of the IEEE 27th International Conference on Data Engineering, April 11-16, 2011, Hannover, Germany, pp: 601-612.

Kalpana, P. and S. Singaraju, 2012. Data security in cloud computing using RSA algorithm. Int. J. Res. Comput. Commun. Technol., 1: 143-146.

Kaur, P. and P.D. Kaur, 2015. Energy efficient resource allocation for heterogeneous cloud workloads. Proceedings of the 2015 IEEE 2nd International Conference on Computing for Sustainable Global Development (INDIACom'15), March 11-13, 2015, IEEE, New Delhi, India, ISBN:978-9-3805-4415-1, pp: 1319-1322.

Liu, Q., G. Wang and J. Wu, 2012. Secure and privacy preserving keyword searching for cloud storage services. J. Network Comput. Appl., 35: 927-933.

Moorthy, V. and S. Sivasubramaniam, 2012. Implementing remote data integrity checking protocol for secured storage services in cloud computing. IOSR. J. Eng., 2: 496-500.

Nagamalli, A., S.S. Krishna and B.K. Priya, 2014. DES security algorithm implementation for cloud computing using counting bloom filter architecture. Can. J. Technol. Innovation, 1: 29-38.

Prasad, P., B. Ojha, R.R. Shahi, R. Lal and A. Vaish *et al*., 2011. 3 dimensional security in cloud computing. Proceedings of the 2011 IEEE 3rd International Conference on Computer Research and Development (ICCRD'11) Vol. 3, March 11-13, 2011, IEEE, Shanghai, China, ISBN:978-1-61284-839-6, pp: 198-201.

Saini, G. and N. Sharma, 2014. Triple security of data in cloud computing. Intl. J. Comput. Sci. Inf. Technol., 5: 5825-5827.

Sharma, T. and V.K. Banga, 2013. Efficient and enhanced algorithm in cloud computing. Int. J. Soft Comput. Eng., 3: 385-390.

Sood, S.K., 2012. A combined approach to ensure data security in cloud computing. J. Network Comput. Appl., 35: 1831-1838.

Takouna, I., E. Alzaghoul and C. Meinel, 2014. Robust virtual machine consolidation for efficient energy and performance in virtualized data centers. Proceedings of the 2014 IEEE International Conference on Internet of Things (iThings), Green Computing Communications (GreenCom) and the IEEE Cyber, Physical and Social Computing (CPSCom), September 1-3, 2014, IEEE, Taipei, Taiwan, ISBN:978-1-4799-5968-6, pp: 470-477.

Thiyagarajan, D. and R. Ganesan, 2015. Data security model employing Hyper Elliptic Curve Cryptography (HECC) and Secure Hash Algorithm-3 (SHA-3) in cloud computing. Intl. J. Technol., 6: 327-335.

Wang, C., N. Cao, J. Li, K. Ren and W. Lou, 2010. Secure ranked keyword search over encrypted cloud data. J. ACM., 43: 431-473.

Xiao, Z. and Y. Xiao, 2013. Security and privacy in cloud computing. IEEE Commun. Surv. Tutorials, 15: 843-859.

Yu, S., C. Wang, K. Ren and W. Lou, 2010. Achieving secure, scalable and fine-grained data access control in cloud computing. Proceeding of the 29th Conference on Information Communications, March 15-19, 2010, San Diego, CA., USA., pp: 1-9.

Zhou, M., Y. Mu, W. Susilo, M.H. Au and J. Yan, 2011. Privacy-preserved access control for cloud computing. Proceedings of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, November 16-18, 2011, Changsha, pp: 83-90.