INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 5 (2016) PAGES 1214 - 1218
RECEIVED : 16/09/2016. PUBLISHED : 21/09/2016
September 22, 2016

A MODIFIED APPROACH TO IMPROVISE THE EFFICIENCY OF DES AND AES USING 1024-BIT KEY

[1]K.Ganesh Shankari, [2]K.Jayasankar,
[1]M.Phil Scholar, Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham,
[2]Asst prof, PG and Research Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham.

Abstract:
The Data Encryption Standard is known as a block cipher technique which means a cryptographic key and an algorithm is applied with a block of data simultaneously rather than one bit at a time. To encrypt a plain textmessage, DES groups it into 64-bit blocks. Each block is enciphered using the secret key into a 64-bit cipher text by means of permutation and substitution.The process involves 16 rounds and can run in four different modes, encrypting blocks individually or making each cipher block dependent on all the previous blocks.

Keywords: DES, cipher text, substitution, encryption.

1. INTRODUCTION

The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding ciphers text to plaintext is called Decryption. This can be done by two techniques symmetric-key cryptography and asymmetric key cryptography.

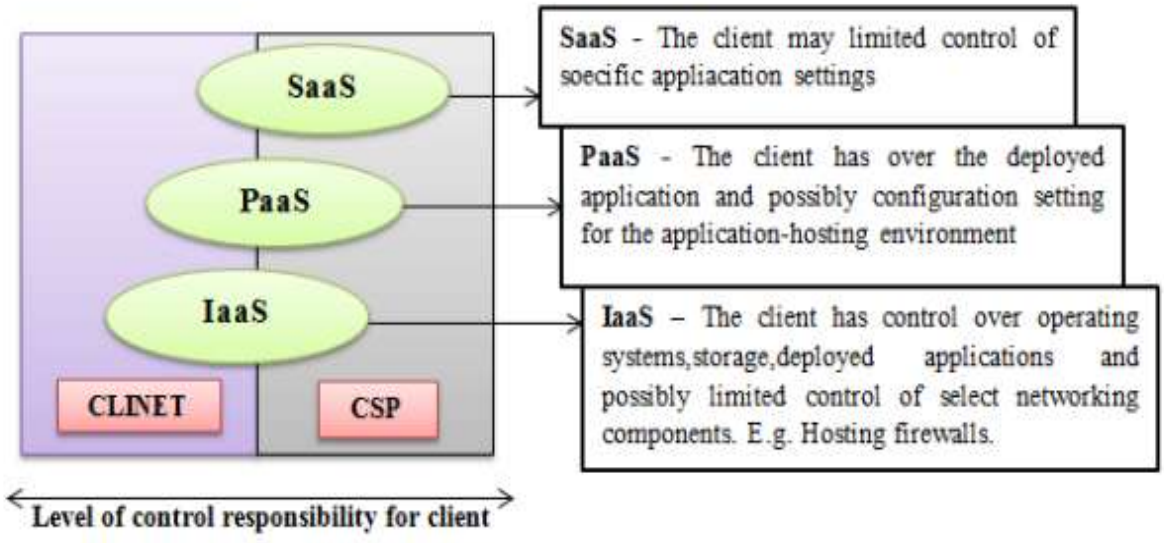

Fig.1. Sample service model

Symmetric key cryptography [3,4,9] involves the usage of the same key for encryption and decryption. But the Asymmetric key cryptography involves the usage of one key for encryption and another, different key for decryption. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms [7,8] etc. and public key cryptography includes RSA, Digital Signature and Message Digest algorithms. For each algorithm there are two key aspects used: Algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic Algorithm

mode). Algorithm mode is a combination of a series of the basic algorithm and some block cipher and some feedback from previous steps.

2. LITERATURE REVIEW

An"Govind Prasad Arya, AayushiNautiyal, Ashish Pant, Shiv Singh &TishiHanda" [4] worked on "A Cipher Design with Automatic Key Generation using the Combination of Substitution and Transposition Techniques and Basic Arithmetic and Logic Operations" proposed Modern computing is observed to be highly dependent on communication and data transport. The security of data during communication has become a mandatory need since the introduction of e-commerce, mails, etc. Moreover a lot of data may be required to be kept secure on local devices also. The encryption of data is the basic requirement today and thus helps to maintain confidentiality of data. A number of algorithms are available for encrypting data while it is transferred from sender to receiver. In this paper we have proposed a cipher which uses basic encryption techniques of substitution and transposition along with application of logic gates, in order to encrypt the data. "Shah Kruti R., BhavikaGambhava" [3] worked on "New Approach of Data Encryption Standard Algorithm" proposed the principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. Within the last decade, there has been a vast increase in the accumulation and communication of digital computer data in both the private and public sectors. Much of this information has a significant value, either directly or indirectly, which requires protection. The algorithms uniquely define the mathematical steps required to transform data into a cryptographic cipher and also to transform the cipher back to the original form. Performance and security level is the main characteristics that differentiate one encryption algorithm from another.

3. PROPOSED WORK

The proposed scheme has first to process the Multiple Rounds for Modified Columnar Transposition Technique (MRMCTT). The plain text message is first converted into the cipher text by using Modified Columnar Transposition Technique as the cipher text is again applied to the columnar technique and for this the cipher will be stronger. Also in every round the enhanced key generation algorithm is applied. The various rounds of MRMCTT may depend upon the security to provide the message. If more security is needed then added more rounds of the MRMCTT scheme and if the normal security then uses minimum 1 or 2 rounds. The input to the MRMCTT is a plain text message and the output is ciphered text message. To apply this scheme we required the matrix or table to perform the encryption process and column number which provide the security key. The output from MRMCTT is then converted into a bit form because the DES algorithm applies its process on bit level as usual. Then the DES has performed its work same as original DES.The security of the algorithm is increased. The Simple Columnar Transposition Technique with multiple rounds is used before DES and the round can be increased and decreased according to need. The Brute Force attack is weak against the Enhanced DES because the intruder required breaking the DES and Simple Columnar Approach both. He required extra time to hack the algorithm.If the intruder is success to hack the key of DES in any way then he required the random number of the columnar approach to reach the plain text successful as well as appropriate remote password authentication scheme with key agreement was proposed. The paper [4] discuss with the view of strong user authentication structure in consideration of cloud computing with a lot of protection characteristics namely; identity management, mutual authentication,session key agreement among the consumer, the cloud server and user kindliness

INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 5 (2016) PAGES 1214 - 1218
RECEIVED : 16/09/2016. PUBLISHED : 21/09/2016
September 22, 2016

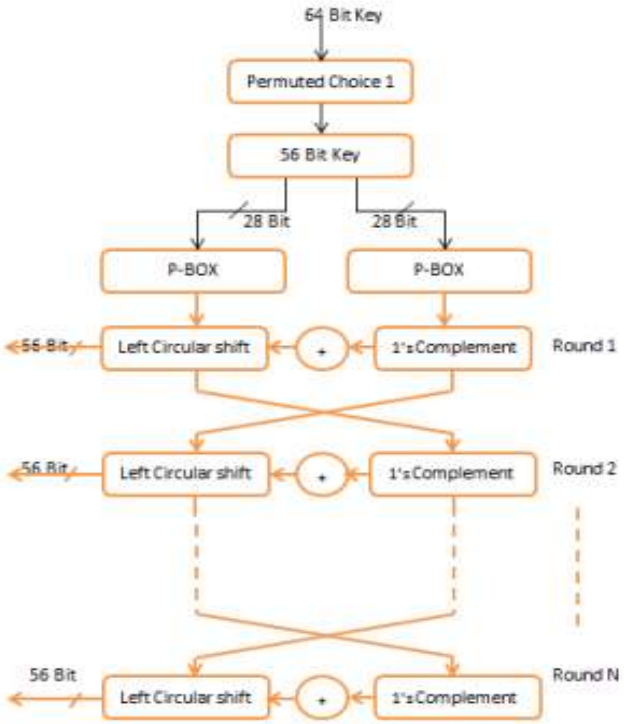

Fig.2. Proposed Enhanced Key generation algorithm flowchart of DES

(i.e, Password modification level). Time-bound ticket-based mutualauthentication scheme isprojectedin paper to overcome the unprotectionto Denial-Of-Service attacks and unconfident password alteration level.

4. ANALYSIS

The paper proposed an authentication protocol suite whichdetect and authenticate cloud users at SaaS layer and providessecureprotection in contradiction of DoS's attack in private cloud. In this private cloud data security purpose,the CSA protocol suite is used which provides authentication security. The CSA protocol suite can be implemented in the SaaS layer of cloud computing systems because the protocol basically relies on fundamental hardware and software provisionsof the cloud systems and cloud users. But when we store the data or images in the public cloud, we need more security for that. Hence, in this work, we have proposed an CSA protocol suite to find a legitimate cloud user's at PaaS layer. But public cloud DIM's we proposed for security purpose, some other techniques(AES, Segmentation, Three Tier Architecture) also.CSA consists of three steps The paper discuss with the AES encryption algorithm for DIM's security in public cloud server. It provides more security and confidentiality of data's as it will increase the key level. Normally AES algorithm gives excellent security for information. AES key size are 128, 192 or 256 bits. Increase in the key level gives strong security in public cloud information. Thereby the hackers never attack the DIM's. After encryption of the DIM's, the paper proposed a segmentation technique. This helps to divide the data to transfer the public cloud server which yields extra security process in the DIM's. The service provider is prevented from "effective" indexing. In commandent the objects of indexing is to run up the analysis of estimated data element across random approach. Once random approach is rejected, indexes will become unusable.consequently, the paper proposed an method

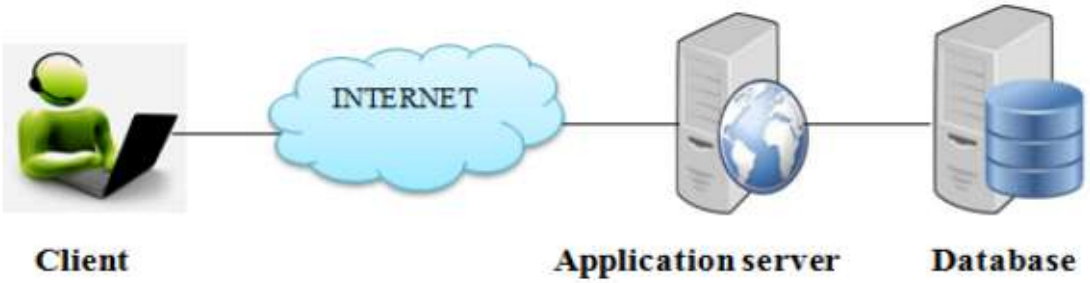

Fig.3. Three Tyre architecture

to deactivate random approach to the data element in the customer's documents. Our method does not trust about connection mechanism policies. The customer specifies visiblyin the policy scheme the management of his data documents and the usage of indexing. The service provider is expected reliable and will notify and consult with the user the keywords to be used for indexing benefits.

CONCLUSION

Based on the study, this paper concludes with improvised performance. Based on author proposed Data and Images (DIMs) Architecture to study and solve the data security problems like authentication,confidentiality, DIMs leakage and transaction in the cloud computing. Nowadays data security is a big challenge task in the public cloud. The Cloud-based Secure Authentication (CSA)Protocol Suite was already implemented in private cloud to handle the DoS attacks both internally and externally using data such as users information only.But still they could not provide an improvised security. Hence,this paper proposes an architecture using CSA protocol inpublic cloud for data with images (DIMs) also.The authors also proposes to introduce an architecture to enhance the security with an AES encryption algorithm by increasing the key size.An increase in the key sizewill provide more security and confidentiality to the client data and the client images (DIMs). Another DIMs security mechanism of partitioning the data and images (encrypted format) to transfer into public cloud server. After the transfer,leakage problems will happen occur in the server side, to handle this an enhanced three tier-architecture protection method is proposed to protect the data and prevents the leakage. As a whole, this paper proposes an enhnaced and an efficient security for DIMs using suitable data and image security techniques such as enhanced AES and, partitioning method in the public cloud.

REFERENCES

1.Pradeep Kumar,K.Selvamani,S.Kanimozhi ,"An Authentication Approach for Data Sharing in Cloud Environment for Dynamic Group" 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT),Vol.pp.262-267,2014.

2. Prashant Rewagad,Yogita,"Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing" 2013 International Conference on Communication Systems and Network Technologies,.pp.437-439,2013.

3.Woei-Jiunn Tsaura,Jia-Hong Lib,Wei-Bin Leeb,"An efficient and secure multi-server authentication scheme with key agreement " The Jurnal of System and Software,Vol.85,Issue 4,pp.876-882,April, 2012.

4. Amlan Jyoti Choudhury, Pardeep Kumar, Mangal Sain, Hyotaek Lim, Hoon Jae-Lee,"A Strong User Authentication Framework for Cloud Computing" 2011 IEEE Asia -Pacific Services Computing Conference,Vol.74,pp.110-115,2011.

5. Jaidhar C.D," Enhanced Mutual Authentication Scheme for Cloud Architecture" 2013 3rd IEEE International Advance Computing Conference (IACC),pp.70-75,2013. 6. M Sulochana,Ojaswani Dubey," Preserving Data Confidentiality using Multi-Cloud Architecture" 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15),Vol.50,pp. 357-362, 2015.