Use of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptographic algorithm to Enhance Data Security in Cloud Computing

Mrs.Mamatha*, Mr.Pradeep Kanchan**

* Department of CSE, NMAMIT, NITTE
** Department of CSE, NMAMIT, NITTE

Abstract- Cloud computing is the relevant technology for this decade. It allows users to store huge amount of data in cloud storage and use as and when required, from anywhere in the world, through any kind of terminal equipment. Since cloud computing relies on internet, cloud data will be forced to contend with security issues like privacy, data security, confidentiality, and authentication. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. This paper, introduces use of hybrid cryptographic algorithm blended with digital signature and Diffie Hellman key exchange.. The hybrid algorithm is designed using the combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of hybrid algorithm makes it tough for hackers to crack the security and integrity of the system, thereby protecting data stored in cloud.

Index Terms- Cloud Computing, AES Algorithm, Data Confidentiality, Hybrid algorithm.

I. INTRODUCTION

Cloud computing is straightforwardly internet computing and the internet is seen as collection of clouds, thus the word cloud computing can be defined as making use of the internet to provide technology enabled services to the needy people and organizations. Many enterprises makes use of cloud computing in order to improve their way of working which implies sharing of computing resources to handle applications. Cloud computing provides services at different abstraction levels, namely Software-as-a-Service (SaaS) ,Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) and also offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability.

Since cloud computing rest on internet, so security issues like user privacy, data theft and leakage, eavesdropping, unauthenticated access and various hackers' attacks are raised. These security issues of authentication, privacy, data protection and data verification are solved by the widespread adoption of cloud computing. Hence to get an overwhelmed acceptance to cloud computing in finance, market and industry as well, we have proposed a secure architecture for it. Under the above mentioned title, this paper incorporates three security control mechanisms via authentication, Encryption and data verification technique in to a single standalone system. Hence it is a three ways protection scheme wherein digital signature is used for authentication, encryption algorithm is used to provide session encryption key and to encrypt user data file, which is to be saved in cloud and to verify integrity of user data trusted computing is used.

A. Need of Hybrid Cryptographic Algorithm

A Computer Network is a group of autonomous computing nodes connected to each other, which uses protocols with mutually agreed set of rules and conventions, to interact with one-another and allow resource sharing among a wide range of users in a predictable and controllable manner. Communication has a major impact on today's business and is desired to communicate data with high security. With the rapid development of network technology, internet attacks are also increased, the traditional encryption algorithms is not sufficient for today's information security over internet, so we propose this hybrid Cryptographic Algorithm.

II. PROBLEM STATEMENT

With cloud computing, organizations can use services and data stored as and when required at any physical location outside their own control. This facility raised the various security issues like privacy, confidentiality, integrity etc., and demanded a trusted computing environment wherein data confidentiality can be maintained. To get rid of the same and to induce trust in the computing, there is need of a system which provides authentication, verification and encrypted data transfer, hence maintaining data confidentiality.

III. PROPOSED SYSTEM

In the proposed architecture, we are using three ways of protection scheme. Firstly, to generate keys for key exchange step, Diffie Hellman algorithm is used. Then digital signature is used for authentication, there after user's data file is encrypted or decrypted using hybrid encryption algorithm. With hybrid algorithm data will be uploaded into cloud server by double encryption .Initially data will be encrypted using AES algorithm and again re encryption will be done by 3DES and similar lily data will be downloaded from the cloud server by decrypting the file as exactly reverse of encryption process. All this is

implemented to provide trusted network at the server end. For the same reason two separate servers are maintained, one for encryption process known as (trusted) computing platform and another known as storage server for storing user data file. When a user wants to upload a file to the cloud server, first key are exchanged using Diffie Hellman key exchange at the time of login, then the client is authenticated using digital signature. Finally user's data file is encrypted using hybrid encryption algorithm and only then it is uploaded to Cloud Storage server. The client can download the same file, from Cloud server. When a user logins, first encryption keys are exchanged, file to be downloaded is selected, authentication takes place using digital signature and hybrid algorithm is used to decrypt the saved file and client is allowed to access the file.

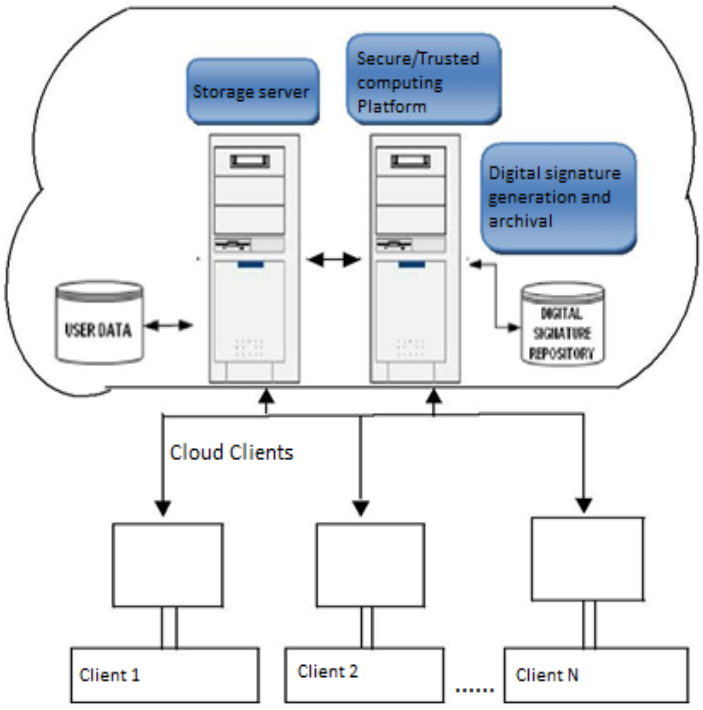


Figure 1: Proposed Architecture

Execution Steps
1. Sign up
2. Login from TCP
   2.1 Key Exchange – Diffie Hellman
   2.2 Digital Signature –SHA-I
3. Uploading / Downloading Data Encryption- Hybrid
4. Data is stored / retrieved from Storage server
5. Logout.

A .Concept of hybrid AES- DES

The idea of a hybrid based AES-3DES can be constructed with reference to basic DES Feistel equations. The repetition of these equations is based on the number of rounds as adapted by the Feistel network, which in the case of DES was standardized for 16 rounds. However, by incorporating the AES within this yields the following results.

L1 =f (R0) ---------- (1)
R1 =AES (f (L0) XOR f (R0)) --------- (2)

The user gives the plain text where the plain text is divided into two halves L0 and R0 of 128 bits each. Each half is then again divided into two halves i.e. LL0 and LR0 from L0 and from R0 we get RL0 and RR0 of 64 bits each respectively. DES algorithm is then applied to all the halves which are generated that is LL0, LR0, RL0 and RR0 using the key given by the user. There is also a provision of using two different keys. If the user selects two keys option at the time of encryption the two different keys are used, one key is used DES encryption and the other key is used for AES encryption. If the user selects one key option at the time of encryption then the same key is used for 3DES and AES encryption. The output of 3DES encryption text is of 192 bits each. Since DES encryption is applied on four quarters each quarter generates an output of 192 bits. The output of LL0 and LR0 is clubbed together to form f (L0) and the output of RL0 and RR0 is clubbed together to form f (R0). The length of f (L0) and f (R0) is 384 bits each. Once we have got f (L0) and f (R0) they both are then XOR with each other i.e. f (L0) XOR f (R0). The length of the output will be same as the length of the input that is 384 bits. The result is then given to the AES algorithm where the result is encrypted using the key provided by the user. The key can be same or different as mentioned above. The output length of the AES encrypted text is 704 bits. The f (R0) can be termed as L1 and the AES encrypted text can be termed as R1. Both L1 and R1 are then clubbed together to give the cipher text of 1088 bits. The Decryption process is exactly reverse of the encryption process.

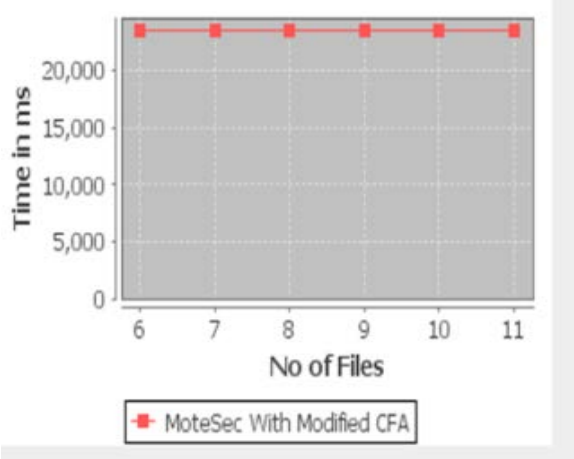
IV. EXPERIMENTAL RESULTS

The hybrid model involves more computations as compared to AES or 3DES alone. The graph shown in (i) specifies the time taken to upload and download data to the cloud server using AES (A) and Hybrid (H) algorithm. For example it takes 142 milliseconds to upload /download file 1 to the cloud server, whereas by using hybrid algorithm it takes 160 milliseconds to upload /download the same file. Hence we can say that the encryption time for the hybrid model is much greater than the time for AES or DES alone. The graph in (ii) and (iii) shows the performance of number of files being uploaded and downloaded with respect to time. The combined effect of uploading and downloading files to the cloud server is shown in the graph (iv). Thus it can be inferred that the hybrid model will take longer time to be broken by the cryptanalyst.

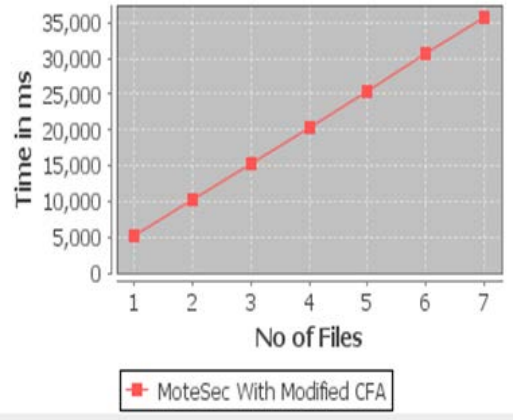
i)Time taken in mili seconds for AES and Hybrid algorithm

A#1#142
H#1#160
A#2#110
H#2#149
A#3#157
H#3#174
A#4#170
H#4#197
A#5#100
H#5#115

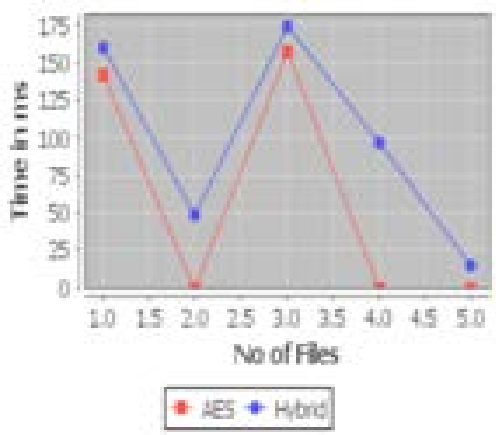
ii) Upload time in ms



iii) Download time in ms



iv) Upload and Download time in ms



V. CONCLUSION

This paper uses combined concept of AES and 3DES to obtain a hybrid model which can be used for uploading the data into the cloud server by encrypting data and downloading the data from cloud server by decrypting the same data. Nowadays as the power of computers is growing day by day, it is very important to design strong encryption algorithms. Thus the hybrid model gives a better non linearity to the plain AES and as it is merged with 3DES, there is better diffusion. Hence the possibility of an algebraic attack on the hybrid model is reduced.

REFERENCES

[1] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[2] Volker Fusenig and Ayush Sharma "Security Architecture for Cloud Networking" 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.

[3] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[4] Sherif el-etriby , Eman m.Mohamed and Hatem s. Abdelkader published "Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing " in the third international conference on communications and information technology ICCIT 2012.

[5] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom "Implementation of Data Security in Cloud Computing" International Journal of P2P Network Trends and Technology- Volume1 Issue1- 2011.

[6] S. Subasree and N. K. Sakthivel: ―DESIGN OF A NEW SECURITY PROTOCOL USING HYBRID CRYPTOGRAPHY ALGORITHMS‖,School of Computing, Sastra University, Thanjavur – 613401, Tamil Nadu, INDIA, February 2010.

AUTHORS

First Author – Mrs.Mamatha, B.E,(M.Tech), NMAMIT,Nitte and salianmamatha@gmail.com.
Second Author – Mr.Pradeep Kanchan, B.E,M.Tech, NMAMIT,Nitte and pradeepkanchan@nitte.edu.in.