Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 6, June-2017

A SURVEY ON VARIOUS CRYPTOGRAPHY TECHNIQUES

Sneha H.R, Mohamed Rafi

DOS in Computer Science and Engineering, UBDTCE Davangere

Abstract - *Secured communication of data is one of the major challenge faced by cloud platforms. It allows a user to store a large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on the internet, security issues like privacy, data security, confidentiality, and authentication are encountered. Inorder to overcome data security issues various encryption techniques are available. To achieve this, we have used Diffie-Hellman key exchange blended with some popular encryption technologies like Advanced Encryption Standard (AES) algorithm .*

Keywords- *Cloud computing, AES algorithm, Diffie-Hellman key exchange, data security issues.*

I. INTRODUCTION

Many organizations today are dependent on cloud platforms for the services they provide. While transferring data between the cloud and organizations there is a possibility of data leakages. This is not acceptable as the data being stored in cloud provider's servers are very sensitive [1]. To overcome such vulnerabilities, various security encryption algorithms have been used to achieve data security with the help of Advanced Encryption Standard (AES) encryption algorithm, Diffie-Hellman Key Exchange algorithm and use of digital signatures [2]. Bi-directional DNA Encryption algorithm is being one such technique to achieve data security. It uses the biological DNA bases ATGC for encoding of messages to achieve data security.

Various encryption techniques have been adopted to achieve maximum data security during transmission. Many firms are unenthusiastic to use cloud services due to data security issues as the data resides on cloud service provider's server. Many researchers choose the best they found and use it in different combination to provide security to the data in the cloud. On the similar terms, we can use the combination of authentication technique and key exchange algorithm blended with encryption algorithm [3].

II. DIFFERENT ENCRYPTION TECHNIQUES FOR SECURED DATA TRANSMISSION

2.1 Use of Digital Signature with Diffie- Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing

In this technique, the author has proposed an architecture where they have used three ways protection scheme. Firstly Diffie-Hellman algorithm is used to generate keys for key exchange step. Then digital signature is used for authentication of the user after that AES encryption algorithm is used to encrypt or decrypt user's data file. All of this is implemented to provide trusted computing environment to avoid data modification at the server end. For the same reason, two separate servers are maintained, one for encryption process known as the (trusted) computing platform and another known as the storage server for storing user data file.

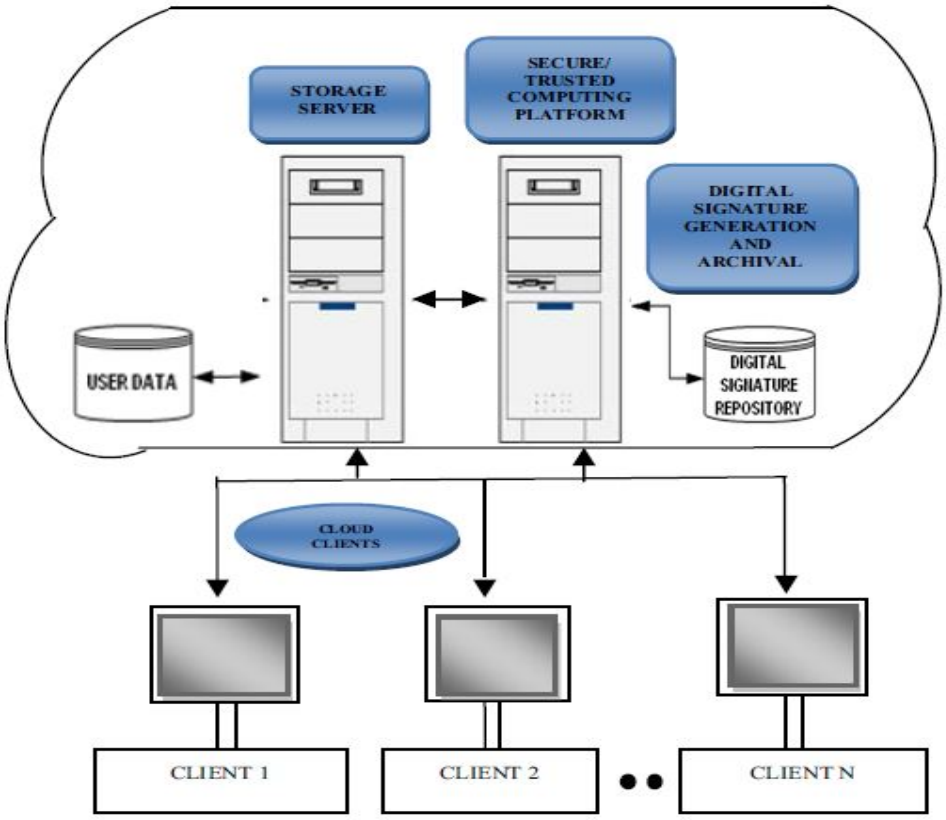

Figure 1: Proposed Architecture

2.2 Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing

Let us assume we have two enterprises A and B. An enterprise A have a public cloud with data, software's and applications. Company B wants a secure data from A's Cloud.We are here, trying to send a secure data to B by using the Digital Signature with RSA algorithm. We are taking some steps to implementing Digital signature with RSA encryption algorithm. Now enterprise A takes data from the cloud, which B wants. Now the data or document is crushed into little line using Hash code function that is called Message Digest. Then A encrypts the message digest within private key the result is in the Digital signature form. Using RSA algorithm, A will encrypt the digitally signed signature with B's public key and B will decrypt the cipher text to plain text with his private key and A's public key for verification of a signature.

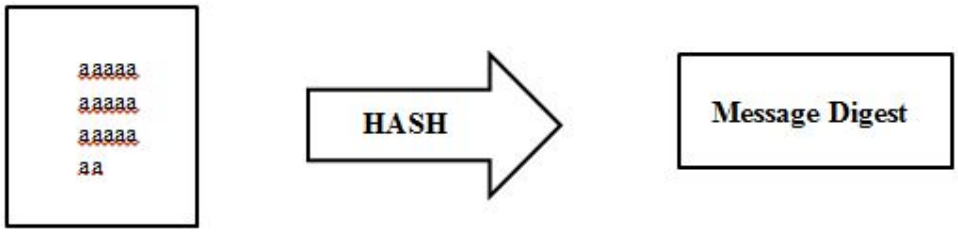

Figure 2 : Document crunched into message digest.

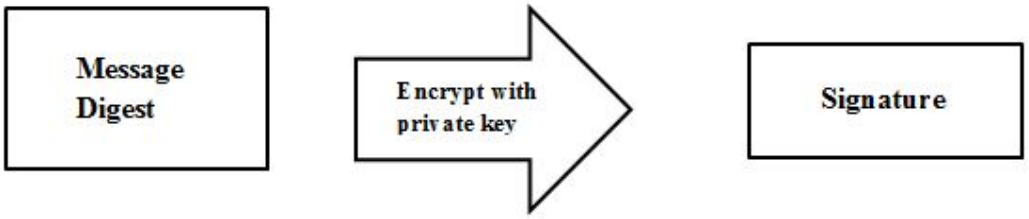

Figure 3: Encryption of message digest into Signature

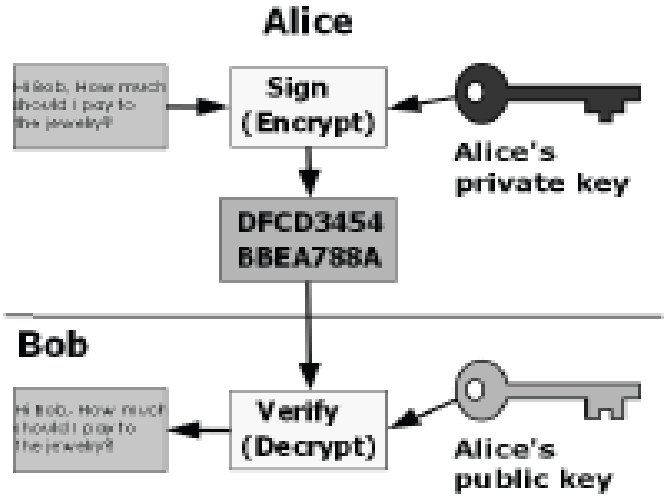

Figure 4: Encryption of Digital Signature into Cipher text

III. ANALYSIS

Each of the encryption algorithms discussed is aiming at increasing the data security when data is transmitted over cloud platforms. Every cryptography techniques concentrate on safety and thereby avoiding the external threats. AES encryption algorithm is used to encrypt the data, and digital signatures are used to authenticate the users. Diffie-Hellman Key exchange algorithm is used for exchanging of secret keys between sender and receiver. Hence data security is achieved to a greater extent and thus avoiding data leakages.

V .CONCLUSION

In this paper, we have reviewed on some of the techniques which are being used for encryption and decryption of data and how it has been implemented. Present methods like AES encryption, Diffie-Hellman Key exchange is used for transferring of secret keys securely and hence ensures security. We have also disused different ways of encoding a message while transmitting in cloud platforms. In this paper, we have mainly concentrated on providing data security in cloud platforms because the data to be stored in cloud is very sensitive hence maximum security has to be achieved by using these techniques.

REFERENCES

[1] PrashantRewagad, YogitaPawar, “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 System and Network Technologies (IEEE ComputerSociety).

[2] Uma Somani, Kanika Lakhani, ManishaMundra, ”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).

[3] Mehdi Hojabri& Mona Heidari“Union of RSA algorithm, Digital Signature and KERBEROS in Cloud Computing” International Conference on Software Technology and Computer Engineering (STACE-2012).