COMPARISON OF SECURITY ALGORITHMS USING SYMMETRIC KEY CRYPTOGRAPHY

[1]Prof. Atiya Kazi,[2] Sayali Ramdas Ghag,[3]Rucha Sanjay Hardikar,[4]Tejal Avdhut Sapte
[1] Assistant professor,[2] Student,[3] Student,[4] Student
[1,2,3,4]Information Technology Engineering,
[1,2,3,4]Finolex Academy Of Management And Technology, Ratnagiri, India

Abstract: Encryption is the technique of hiding private or sensitive information within something that appears to be nothing be a usual. If a person views that cipher text, he or she will have no idea that there is any secret information. Encryption performs a major role to intelligently misguide humans by not actually making the data visible to them but wrap it in the form that humans cannot detect the inside data. This system enables the user to send their secret text on cloud by providing a key to them. This key encrypts the data so that even if the data is grabbed by the hacker, it won't be disclosed. The receiver uses the shared secret key which was used by the sender, to decrypt the received message. For providing more security comparison of Diffie-Hellman key exchange, Data Encryption standard (DES) and Blowfish is done. This will offer the better algorithm for providing security of both as it uses public key techniques to allow the exchange of a private encryption key. This method ensures that the secret message is sent over cloud securely. If sender sends this cipher text in public others will not know what is it, and it will be received by receiver. The cloud data storage is used to store the required information. The project will be primarily accessing the output stored on cloud for comparing purpose.

Index Terms - Diffie-Hellman, DES (Data Encryption Standard), Blowfish, Cloud Computing

I. INTRODUCTION

Encryption is the process of hiding or encoding a message in a way that authorized person can access the data or information or else the data cannot accessed the unauthorized person. In an encryption two terms are mainly consider such as plaintext and cipher text .A plaintext is an original message and a cipher text will be an encrypted message that can read only when it can be decrypted. There are basically two types Symmetric key and Asymmetric key .Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks. Primarily, Encryption is used to protect the data of online transactions and other confidential information from acknowledging from the radar of hackers. Decryption is the reverse process of encryption .The cipher text message will be decrypted and we get the original message. Decryption it requires a secret key. Decryption with the correct key is simple. Decryption requires a correct key, without which the encrypted data cannot be unlocked.. Data transfer on cloud is privileged by the users but the major drawback is information security. To overcome this issue we can use DES and Blowfish security algorithms with the help of keys generated in Diffie-Hellman Key exchange algorithm as input. Diffie-Hellman key exchange algorithm ensures transfer of information in secured environment.

II. LITERATURE SURVEY:

2.1 In this paper Secure Socket Layer (SSL) is a cryptographic protocol develop by Netscape. For providing High security on Network Diffie-Hellman Key Exchange protocol are implemented with the help of Secure Shell(SSH).Basically SSH is consider as a protocol and also a program which is used to encrypt traffic between two computers[5].

2.2 A study of encryption algorithms (RSA, DES, 3DES, and AES) for Information security. With the fast growth in digitalization in data exchange, information security is a much necessary in data storage and transformation. Encryption is the process of encoding a message in such a way that only the intended recipient can read it. Encryption is way that provide a means for securing the information. Encryption algorithm performs various operations on plaintext and transforms it into cipher text which is decrypted at the receiver site to generate the plain text(Original message).During encryption one key(numeric or alpha-numeric text or a special symbol) is used and the same key is used to decrypt the same. It is called as Symmetric Encryption.DES is a Block cipher and uses Symmetric key Cryptography. It encrypts and decrypts blocks of data consisting of 64 bits by using a 64-bit key.DES, despite of growing concerns about vulnerability, is still widely used by financial services and other industries worldwide to protect sensitive online applications. The algorithm heads with an initial shuffling of sixteen rounds block cipher and a final permutation. There are many attacks and methods that exploit the weaknesses of DES, which makes it an insecure block cipher [7].

2.3 Comparative analysis of AES and DES security Algorithms. Cryptography is a process that makes it possible for two peoples to exchange message secretly in such a way that a third person cannot understand the same. The original message is called the "plain text" and a encrypted message is called the "cipher text". Cryptography is where security engineering meets mathematics. This methods has often been used to protect the confidential information. Symmetric Key, Asymmetric key and Hash functions are the existing three types of cryptosystems. Also there are many security algorithms out of which DES is a symmetric key cryptographic algorithm that uses single key for both encryption and decryption [8].

2.4 Design and Simulation DES of encryption for information security. In this paper the demand for protection of data increases, when the confidentiality has very high value. Security is very necessary thing in order to avoid unauthorized access by third party user. The remedy or solution for this issue is Cryptography. It's the art of secret writing, which authenticates data as well as important messages and protects the system from valid attacks. DES has been the most extensively used encryption algorithm standard in recent times [1].

2.5 In this paper we studied that by using Authentication how security has been provided. The authentication has been provided by using Diffie -Hellman key exchange algorithm .By using Authenticated key agreement it provides authentication of both communicating parties and establish a secure session key. The major disadvantage of this paper such as MESDHP (modified computational D-H problem).This scheme reduced the number of modular exponentiations but did not protect the client [2].

2.6 In this paper consider discussion over a how to avoid unauthorized access. Basically sending any information from sender to receiver, the receiver can receive the original information or data without any unexpected change which will be made by unauthorized person. For providing a more security we will use the secret key to encrypt the original message. The secret key will generated by using Diffie-Hellman key exchange. The main advantage of this paper is it has been avoid a man-in-the-middle – attack or try to reduce the chance of occurring the man-in-the-middle attack [9].

2.7 In this paper the Cloud and Digital Signature this are important factor .Cloud it allows to user to store the huge amount of Data in the storage. Since cloud computing relies the most security issues like privacy, data security, confidentiality, and authentication. For providing more security use of hybrid cryptographic algorithm with digital signature and Diffie Hellman key exchange. Basically hybrid cryptography is combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithm to protect confidentiality of data stored in a cloud [4].

2.8 A comparative study for throughput of Encryption algorithm for text, image, audio and video files concluded that blowfish algorithm has a better performance than DES and 3DES .Primarily blowfish is a variable length key, 64 bit block cipher comprising of two important parts firstly an expansion part and the next is data encryption part where the latter occurs via Fiestal network. In the proposed system, for more security, additional keys are added to increase the length of the key and given as input to hash function for increasing the robustness of Blowfish algorithm. [10] Blowfish is one of the type of symmetric key algorithm having shared secret key where same key is used for both encryption and decryption [6]

2.9 Information security is achieved using Blowfish algorithm for enhanced network security and defence applications. The paper primarily focuses on reducing the rounds of algorithm VHDL language is incorporated in the design simulation of the project done by Xilinx ISE software. For applications comprising of small key size, large number of iterations get superfluous due to the tradeoff between the complexity of attacks, that help in reducing number of iterations without loss of security.[3]

III. PROPOSED SYSTEM:

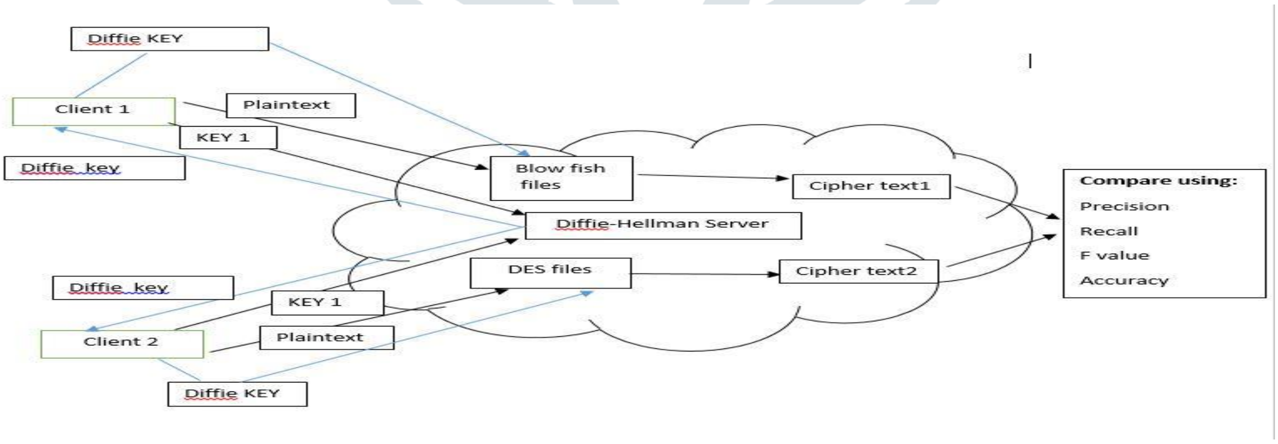

Figure 3.1: Proposed system

In this system, the key of both the clients that want to share data on cloud is given as an input to the Diffie Hellman algorithm that generates a shared secret diffie key.

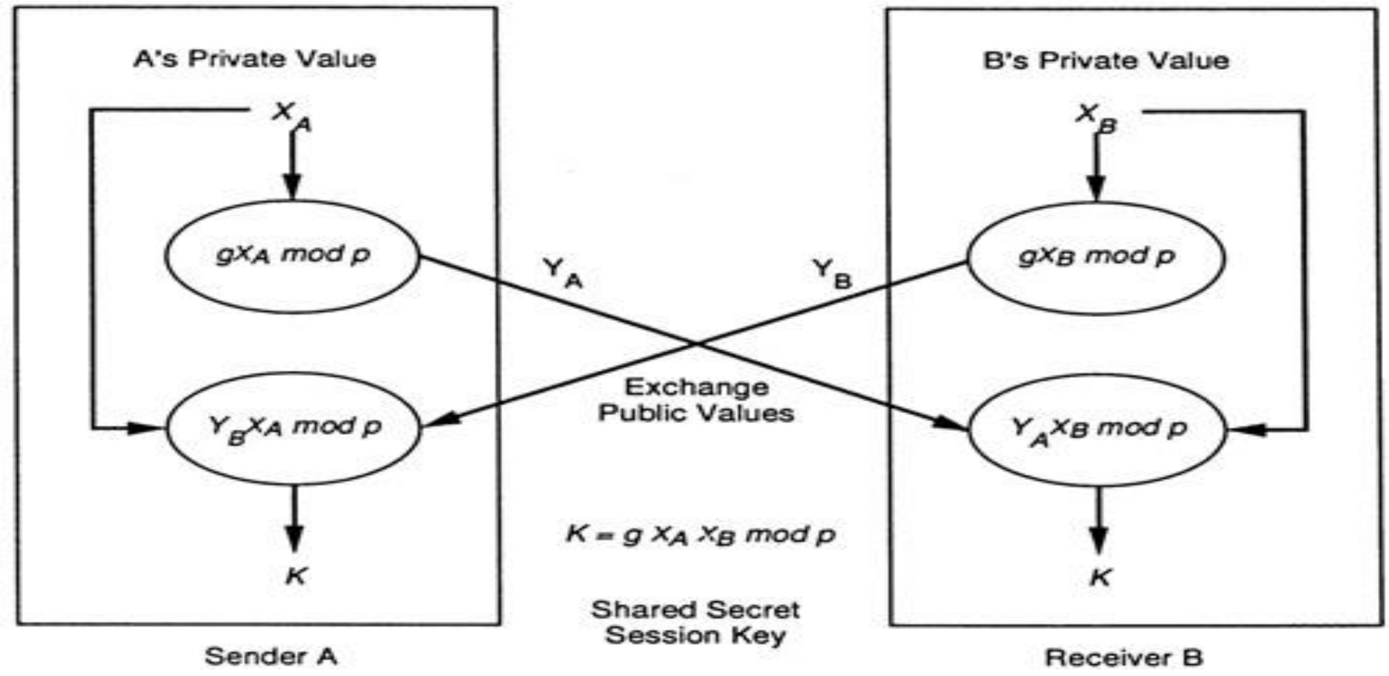

Figure 3.2: Diffie Hellman algorithm

This key is sent back to the clients and the clients then send the diffie key as a key for encryption to DES and blowfish algorithm. After encryption, the cipher text is generated. This cipher text is compared on the basis of the parameters like precision, fvalue, accuracy and recall.

IV.CONCLUSION :

The major issue for uploading data on cloud is about information security. This the proposed system has used the method of comparative study to analyze exactly which algorithm provides better security. The comparison of algorithms is done on certain specified parameters like precision, recall, fvalue and accuracy. The result of this study can help to build a system using the better algorithm to provide more secure data transfer on cloud. The proposed system uplifts the level of security as it uses Diffie Hellman algorithm to generate a shared key and the DES and Blowfish algorithms are checked for its performance of generating the secured cipher text.

V. REFERENCES:

[1] Design & simulation DES algorithm of encryption for information security Mohammad A. Hameed Ahmed I. Jaber 2018.
[2] Authenticated Diffie Hellman key agreement scheme that protects client anonymous and achieves half forward secrecy Hung Yu Chien 2015.
[3] Blowfish encryption algorithm for Information Security Sai Kumar Manku and K. Vasanth 2015.
[4] 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 2015 .
[5] A study of diffie Hellman algorithm in network security Vinothini Sarany Vasumathi 2014.
[6] Blowfish Algorithm Neha Khatri Valmik VK. Kshirsagar 2014.
[7] Study of encryption algorithm RSA, DES 3DES for information security Gurpreet Singh Supriya 2013 .
[8] Comparative analysis of AES and DES security algorithm Sumitra 2013 .
[9] On a key exchange technique avoiding the man in the middle attack Barun Bishwas Krishnendu Basuli Samar Sen Sarma 2012.
[10] Study of new trends in blowfish algorithm Gurjeeran Singh Ashwani Kumar K.S Sandha 2008.