Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.265 – 270

RESEARCH ARTICLE

Triple Encryption Method on Password for Secured Cloud Data Storage in Mobile

S.UMADEVI@YASODHEI, D.NIRMAL DEV, K.SAKTHIVEL

Computer Science & Engineering (CSE), IFET College of Engineering, India

Abstract— Cloud Computing is a new era in the world of computer. Cloud computing is a recently evolved computing terminology or metaphor based on utility and consumption of computing resources. Cloud computing is based on client-server architecture. Cloud computing involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer services or resources.it is highly vulnerable because in last 3 months itself 10 celebrities private cloud server has been hacked due to many issues like data authenticity , integrity , data hiding and availability. In this paper we introduce a mechanism to provide secure data. We combine two algorithm Blowfish and AES to provide security to password and data in cloud computing.

Index Terms— Cloud computing, Blowfish, AES

I. INTRODUCTION

Cloud computing is a term which is used to refer a model of network computing where a program or application runs on a connected server or servers rather than on a local computing device such as a PC, like the traditional client server model. Cloud computing relies on sharing of resources to achieve coherence of network. Cloud computing have aimed to allow access large amounts of data in a fully virtualized manner. Cloud computing allows for the sharing and scalable deployment of services from almost any location, for which the customer can be charged based on actual usage .Security is needed against unauthorized access and to reduce risks of data stealing. Cloud provider hosting a large set of databases to their customer and by securing cloud means that storage should be protected and secured for the privacy purpose. In this paper we will focus the security of data in cloud computing
– How data is to be secure on cloud.

II. SECURITY IN CLOUD COMPUTING

Cloud computing provide several services to their clients. cloud computing is a huge collection of inter connected network. So main challenge is to provide security to cloud network. There is number of security concern associated with cloud computing. The main aim of security is to provide availability, confidentiality, integrity to the data. There are so many risk associated with the cloud network like data can be hacked by an unauthorized person. Data can be changed by third party while transferring the data. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. In this paper we will use 'Triple Encryption of password in Cloud Computing' by using two different security algorithms such as-

1) Advanced Encryption Standard
2) Blow Fish

III. METHODS OF SECURITY IN CLOUD COMPUTING

A. Advanced Encryption Standard (AES)

AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijndael, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES became effective as a federal government standard on May 26, 2002 after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module (see Security of AES, below).

High-level description of the algorithm

- KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

- InitialRound
  - AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
- Rounds
  - SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
  - ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
  - MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
  - AddRoundKey. Final Round (no MixColumns)
  - SubBytes
  - ShiftRows
  - AddRoundKey.

Until May 2009, the only successful published attacks against the full AES were side-channel attacks on some specific implementations. The National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for U.S. Government non-classified data. In June 2003, the U.S. Government announced that AES could be used to protect classified information.
AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. By 2006, the best known attacks were on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys.

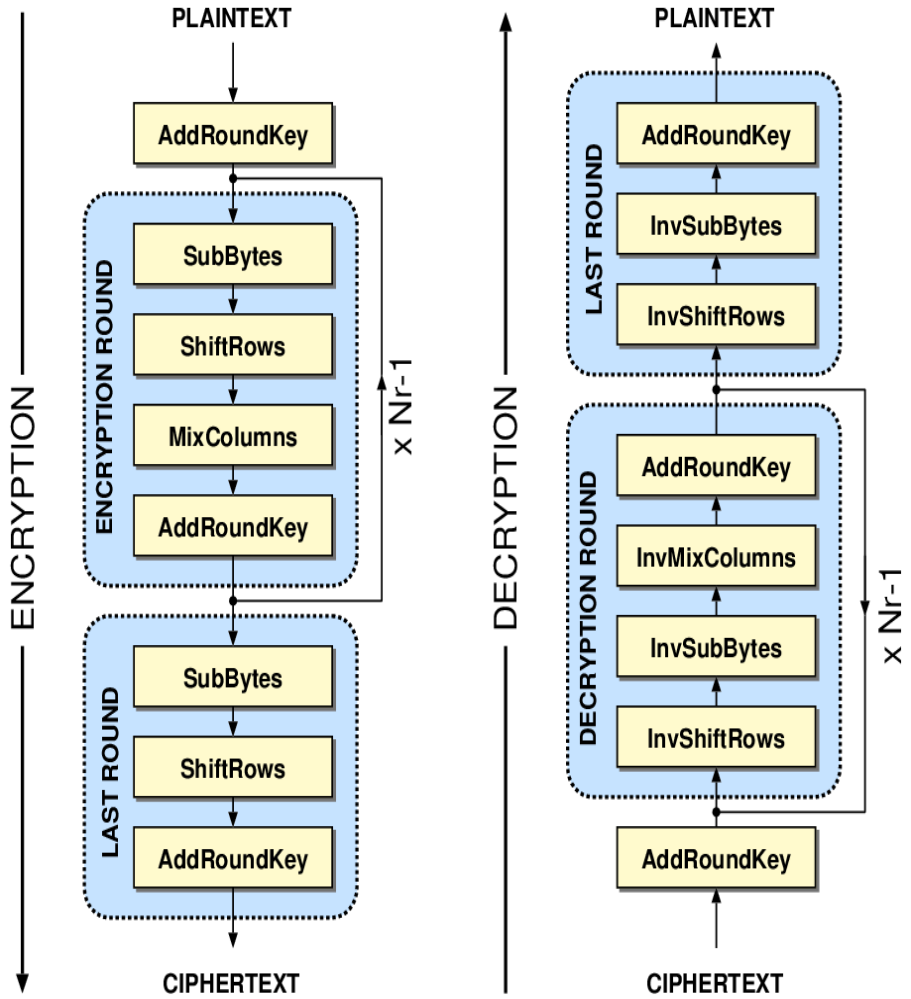

Figure – 1 AES Architecture

Performance

High speed and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware, from 8-bit smart cards to high-performance computers.

1.On a Pentium Pro, AES encryption requires 18 clock cycles per byte, equivalent to a throughput of about 11 MB/s for a 200 MHz processor. On a 1.7 GHz Pentium M throughput is about 60 MB/s.

2. On Intel Core i3/i5/i7 and AMD APU and FX CPUs supporting AES-NI instruction set extensions, throughput can be over 700 MB/s per thread.

B. Blowfish Algorithm

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure it resembles CAST-128, which uses fixed S-boxes.

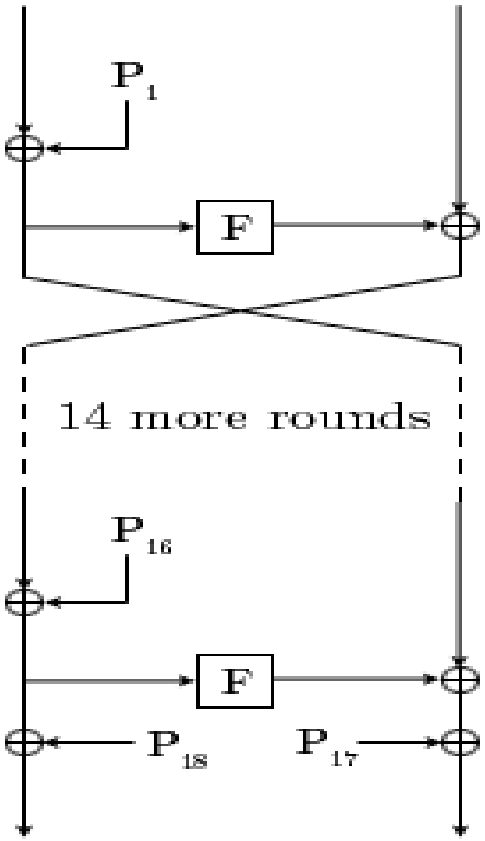

Figure – 2 The Feistel structure of Blowfish

Blowfish's key schedule starts by initializing the P-array and S-boxes with values derived from the hexadecimal digits of pi, which contain no obvious pattern (see nothing up my sleeve number). The secret key is then, byte by byte, cycling the key if necessary, XORed with all the P-entries in order. A 64-bit all-zero block is then encrypted with the algorithm as it stands. The resultant ciphertext replaces P_1 and P_2. The same ciphertext is then encrypted again with the new subkeys, and the new ciphertext replaces P_3 and P_4. This continues, replacing the entire P-array and all the S-box entries. In all, the Blowfish encryption algorithm will run 521 times to generate all the subkeys - about 4KB of data is processed.

Because the P-array is 576 bits long, and the key bytes are XORed through all these 576 bits during the initialization, many implementations support key sizes up to 576 bits. While this is certainly possible, the 448 bits limit is here to ensure that every bit of every subkey depends on every bit of the key, as the last four values of the P-array don't affect every bit of the ciphertext. This point should be taken in consideration for implementations with a different number of rounds, as even though it increases security against an exhaustive attack, it weakens the security guaranteed by the algorithm. And given the slow initialization of the cipher with each change of key, it is granted a natural protection against brute-force attacks, which doesn't really justify key sizes longer than 448 bits.

IV. OVERALL DESIGN OF PROPOSED WORK

In our proposed work we provide security by implementing two algorithm Blowfish and AES together to cloud network. To implement these three algorithm we use Asp.net as a platform.

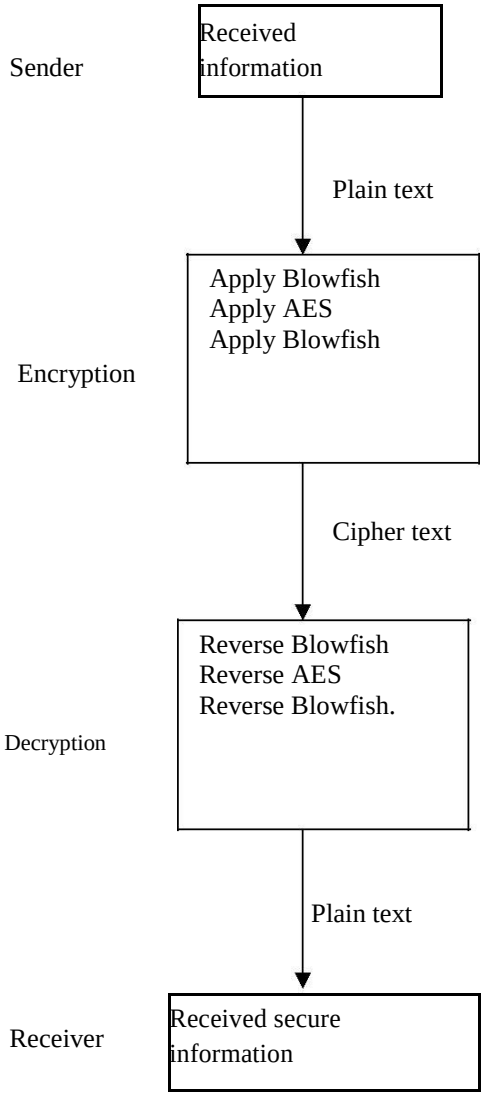

Figure – 3 Overall system design

In our proposed system for encryption first apply Blowfish for authentication of data. Then apply AES algorithm for encryption and then hiding data within second encryption in blowfish for provide maximum security to the data. Receiver can get original plain text by reversing the AES and 2 * Blowfish.

V. CONCLUSION AND FUTURE WORK

In this paper we implement Blowfish Algorithm and Advanced Encryption Standards to provide maximum security in cloud computing. By implementing these two algorithm we provide authenticity, security and data integrity to the data. We try to improve the time complexity by using these security algorithms to some extent.

REFERENCES

[1] Garima Saini, "Triple Security of Data in Cloud Computing"
In International Journal of Computer Science and Information Technologies, Jun-2014.

[2] Chao Yang, "A novel triple Encryption Scheme for Hadoop based cloud computing", in Emerging intelligent data and web technologies, IEEE, Sep- 2013.

[3] Patidar, S "Survey on cloud computing", in Advanced computing and communication technologies , IEEE , Jan- 2012..

[4] M. Vijayapriya, "Security algorithm In Cloud Computing: Overview"/ International Journal of Computer Science & Engineering Technology(IJCSET)

[5] Rashmi Nigoti, Manoj Jhuria & Dr. Shailendra Singh," A Survey of Cryptographic algorithms for Cloud Computing.In International Journal of Emerging Technologies in Computational and Applied Sciences(IJETCAS), ISSN(print) 2279-0047, ISSN(online):2279-0055.

[6] B.Arun & S,K. Prashanth, " Cloud Computing Security Using Secret Sharing Algorithm" in Indian Journal of Research, ISSN-2250-1991, Volume:2|Issue: 3| March 2013.

[7] Approach to Hide Text in Images Using Steganography"
In International Journal of advanced Research in Computer Science and software Engineering, ISSN: 2277 128X, Volume 3, Issue 4, April 2013.

[8] V.K. Zadiraka & A. M. Kudin, " Cloud Computing In Cryptography And Steganography", in Cybermetics and Systems Analysis, Vol. 49, No. 4, July-2013, UDC 681,3;519,72;003,.26.

