ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 7, Issue 10, October 2018

Using Different Encryption Techniques for Balancing with Cluster-Based Storage

Annie p Joseph[1], Ciya James[2]

Assistant Professor, Dept. of ECE, Jyothi Engineering College Cheruthuruthi, Thrissur, Kerala, India[1]

PG Student, Dept. of ECE, Jyothi Engineering College Cheruthuruthi, Thrissur Kerala, India[2]

ABSTRACT: As communication is widely through internet data security is an essential area of concern. To send the secret data more securely the data is hidden inside image, audio, video, text etc. As more and more information is stored on computers or communicated via computers, the need to insecure that is information is invulnerable to snooping or tampering becomes more relevant. Cluster based storage is a group of nodes that are linked together where each node is assumed as server. People today are so addicted to the internet that they can't live without it. This addiction has lead to a massive demand of internet services; it's been observed that internet traffic has been increasing rapidly, causing a large delay in server response time . To control this delay or to reduce the load from servers, four different encryption techniques and cluster based storage are used. By using these techniques, they not only reduces the load from the server, but it also shows which server takes less time to fulfill any requests by showing the response time of each server. Information Confidentiality has a prominent significance in the study of ethics, law and most recently in information systems. Encryption can provide a means of securing information. A survey of various encryption techniques, Hybrid Rivest Shamir Adelman (HRSA),Digital Signature Algorithm (DSA), Triple Data Encryption Standard (TDES), Advanced Encryption Algorithm (AES) which used to reduce the server load and comparisons are also done between these encryption techniques in order to show the best encryption technique**.**

KEYWORDS: HRSA, DSA, AES, TDES, cryptosystem, Encryption, Decryption

I. INTRODUCTION

Due to the wide use of internet the communication is mainly through internet. So security must be ensured while transferring the data through internet, since the intruders mainly focuses on this type of communication. Different techniques has been developed to transfer the secret data. The most important tehcniques are Hybrid rivest shamir adleman, Digital signature algorithm, Triple date encryption standard and Advanced encryption standard. Here mainly explains about the security and control the delay or to reduce the load from servers. But it also shows which server takes less time to fulfil any requests by showing the response time of each server. Security is the mechanism by which information and services are protected from unintended or unauthorized access, change or destruction. Security in networking is based on Cryptography (a word with Greek origins, means “secret writing”), the science and art of transforming messages to make them secure and immune to attack.

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption. A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together. Asymmetric encryption techniques are about 1000 times slower than Symmetric encryption which makes it impractical when trying to encrypt large amounts of data. Also to get the same security strength as symmetric, asymmetric must use a stronger key than symmetric encryption technique. The distributed cluster based storage is used, which in turn is working as a server. There are three different encryption techniques that play a very vital role in the process Hybrid rivest shamir Adelman, Digital signature algorithm, Triple date encryption standard and Advanced encryption standard. The use of these techniques eventually leads to a reduction of the server load

DOI:10.15662/IJAREEIE.2018.0710006

II. LITERATURE SURVEY

There are many cryptographic algorithms available in the mark to encrypt the data. The strength of encryption algorithm heavily relies on the computer system used for generation of keys. Some encryption algorithms are discussed below:

HYBRID RIVEST SHAMIR ADLEMAN(HRSA)

Hybrid encryption is a combination of symmetric and asymmetric encryption methods. Symmetric algorithms are used for encryption of messages rather than asymmetric. Thus, the asymmetric algorithm RSA is used for the purpose of safeguarding and protecting the data[1]. The secret key which solves the problem of key exchange can be sent securely. Database encryption is the process of converting data within a database. That is, the plain text (Readable) format is converted into a cipher text (Unreadable format) using keys generated

by the encryption algorithm. Database decryption is converting the cipher text into the Plain text (original information) using keys generated by the encryption algorithms. Database encryption can be provided only in file format or column format. The encryption is playing a vital role in database management systems. Only the encrypted files are stored in their database. The database security is the mechanism that protects the database against intentional or accidental threats. The encoding of the data by a special algorithm that renders the data unreadable by any program without the decryption key.

DIGITAL SIGNATURE ALGORITHM (DSA)

The Digital Signature Algorithm (DSA) has been developed by the accredited standards committee on financial services as part of standard x9.30-1997: Public Key Cryptography using irreversible algorithms for the financial services industry. That standard consists of two parts.

Part 1: Digital signature algorithm

Part 2: secure hash algorithm

The Digital signature algorithm has been suggested and standardized by the national institute of standard and technology[2] . It is an efficient variant of the ElGamal signature scheme. ElGamal signatures scheme has several draw backs which the DSA repairs. The DSA defines technique for generating and validating digital signatures. This technique is supposed to provide data integrity and non-repudiation of the origin and content of a digital message. The authenticity of many legal, financial, and other documents is done by the presence or absence of an authorized handwritten signature. “Digital Signature” is the best solution for authenticity in various fields. A digital signature is nothing but an attachment to any piece of electronic information. Which represents the content of the document and the identity of the owner of that document uniquely. Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document. The overall process of digital signature standard as shown in the Fig.2 .Digital Signature of a person therefore varies from document to document .Ensuring authenticity of each word of that document. As the public key of the signer is known, anybody can verify the message and the digital signature.

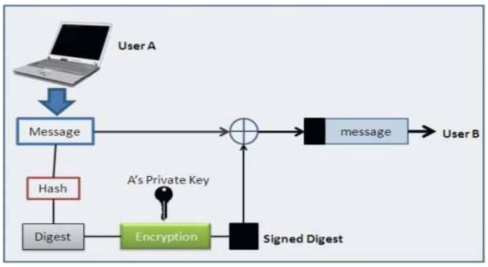

Fig.1 Block Diagram Of Digital Signature Standard

signature scheme[4]. Therefore, no rigorous security proofs for signature schemes are known and Three main important steps are : Digital Signature Generation, verification and secure hash algorithm.

The DSA is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature generation process and the public key is used in the signature verification process. For both signature generation and verification, the data (which is referred to as a message) is reduced by means of the Secure Hash Algorithm (SHA) specified in FIPS 180-1[3]. An adversary, who does not know the private key of the signatory, cannot generate the correct signature of the signatory. In other words, signatures cannot be forged. However, by using the signatory's public key, anyone can verify a correctly signed message. Secure Hashing Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. A hash function, is a function that takes some message of any length as input and transforms it into a fixed-length output called a hash value, a message digest, a checksum, or a digital fingerprint. A hash function is a function f : D → R, where the domain $D = \{0, 1\} *$, which means that the elements of the domain consist of binary string of variable length; and the range $R = \{0, 1\} n$ for some $n \geq 1$, which means that the elements of the range are binary string of fixed-length. So, f is a function which takes as input a message M of any size and produces a fixed-length hash result h of size n. A hash function f is referred to as compression function when its domain D is finite, in other word, when the function f takes as input a fixed-length message and produces a shorter fixed-length output.

The security of all known digital signature schemes depends on the intractability of certain computational problems in mathematics, specifically in number theory. in the case of DSA ,The group is subgroup of prime order in the multiplicative group of a finite prime field. However ,no provably hard computational problems are known which can serve as the security basis of a digital there is little hope that such proofs will be found in future. Today's security proofs are reductions. This goal of such reduction is to show that the ability of an attacker to mount a successful attack on a signature scheme implies his ability of solving basic computational problem in mathematics. This is supposed to increase the trust in the security of a digital signature system.

TRIPLE DIGITAL ENCRYPTION STANDARD (TDES)

To provide strong protection against certain attacks (dictionary attacks and matching cipher text attacks) which exploit the DES block size of 128 bits(with parity, 112 bits without parity). We are also using three keys (64 bits each) in the project which are independent of each other. We are first encrypting the input data (Plain text) with first key, then decrypting the output with the second key and again encrypting it with the third key. These make our data three times more stronger than the earlier algorithm i.e. DES. This algorithm was needed after the crack of DES in mid 90's.

Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits (without parity) was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

The encryption algorithm is:

Cipher text = EK(DK(EK(plaintext)))

Decryption is the reverse:

plaintext = DK(EK(DK(cipher text)))

Encrypt -the plaintext, firstly using key k1, followed by encryption with key k2, a third encryption is carried out with key k3. 3DES uses three keys to provide a high level of security. It shown in Fig.2

DOI:10.15662/IJAREEIE.2018.0710006

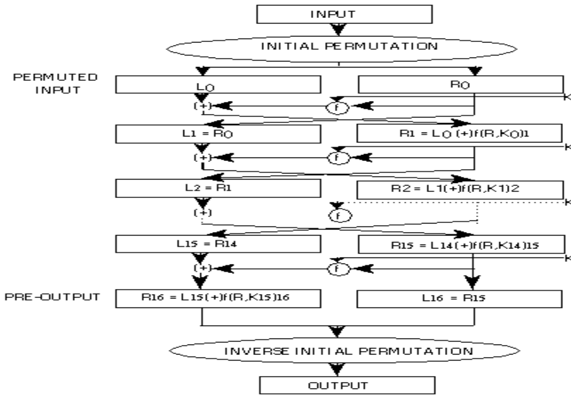

Fig.2 Triple DES with 3 key

In general, Triple DES with three independent keys (keying option 1) has a key length of 168 bits (three 56-bit DES keys), but due to the meet-in-the-middle attack, the effective security it provides is only 112 bits. Keying option 2 reduces the effective key size to 112 bits (because the third key is the same as the first). However, this option is susceptible to certain chosen-plaintext or known-plaintext attacks, and thus, it is designated by NIST to have only 80 bits of security. The best attack known on keying option 1 requires around 232 known plaintexts, 2113 steps, 290 single DES encryptions, and 288 memory (the paper presents other tradeoffs between time and memory). This is not currently practical and NIST considers keying option 1 to be appropriate through 2030. If the attacker seeks to discover any one of many cryptographic keys, there is a memory efficient attack which will discover one of 228 keys, given a handful of chosen plaintexts per key and around 284 encryption operations.

The DES and TDES devices are used by the federal department and other government agencies for cryptographic protection of classified information. The federal government

standardizes DES and specifies interoperability and security-related requirements for using encryption at the Physical Layer of the ISO Open Systems Interconnection (OSI) Reference Model in telecommunications systems conveying digital information. In addition to Preserving confidentiality, cryptography can be used for:

- Authentication: the receiver of the message can ascertain its origin
- Integrity: the receiver can verify if the message was modified during the transmission
- Non-repudiation: the sender cannot deny that she sent the message

The DES and TDES cores are very compact cores[5]. Encryption cores are typically implemented with data and key buses connected to other modules internal to the FPGA. Data encryption (and particularly DES) is primarily applied in:

- Electronic financial transactions: Automatic Teller Machines (devices limited to the issuance of cash or travelers checks, acceptance of deposits, or account balance reporting)
- Secure data communications, paving the road for e-commerce
- Secure video surveillance systems
- Encrypted data storage and proprietary software protection
- Access control: Software or hardware which protects passwords or Personal Identification Numbers (PINs) against unauthorized access.

The DES and TDES functionality is usually integrated within embedded systems. Triple-DES is prevalent in Fax machines. This allows secure data transfer over phone lines and prevents active interception of one's faxes at the receiver end, which is prevented by password entry by the user for fax retrieval. Networking applications use DES and Triple- DES to provide network protection through data privacy, data integrity, access control and authentication. Message and file security, user authentication, secure remote system logon, and multilevel system access require data encryption, and DES and Triple-DES algorithms are the most prevalent.

ADVANCED ENCRYPTION STANDARD (AES)

AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text . AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an Add Round Key stage. However, before reaching the final round, this output goes though nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key. In the final (10th) round, there is no Mix-column transformation [3, 20]. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.

III. . COMPARITIVE STUDY OF DIFFERENT ENCRYPTION ALGORITHMS

In the Table 1below a comparative study between AES, TDES , HRSA ,DSA is presented in to eighteen factors, which are Key Size, Block Size, Ciphering & Deciphering key, Scalability, Algorithm, Encryption, Decryption, Security, Deposit of keys, , Key used, Rounds, Stimulation Speed, and Ciphering & Deciphering Algorithm.

	HRSA	AES	DSA	TDES
Block size	64 BIT	128 BIT	64 BIT	64 BIT
Key size	1024 BITS	128,192,256 BIT	1024 BIT	168 BIT
Algorithm Structure	Router level network topology	Substitution, permutation network	Hash Algorithm structure	Feistel network
Rounds	1	9.11.13	16	48
Security Attacks	Least secure	Side channel attacks	Any computer user. error free	Adequate security
Cipher Type	Asymmetric block cipher	Symmetric Block cipher	Asymmetric block cipher	Symmetric block cipher
Algorithm	Asymmetric	Symmetric	Asymmetric	Symmetric

DOI:10.15662/IJAREEIE.2018.0710006

Key	Different keys are used of encryption and decryption	Same key used	Different key used	Different key used
Speed	Slowest	Very fast	Normal	Very slow

Table 1 : Comparison Between Different Encryption Techniques

Encryption algorithm plays very important role in Communication security. Our research work surveyed the performance of existing encryption techniques like AES, TDES, DSA and HRSA algorithms. So there are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used . To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own pro’s and con’s. According to research done and literature survey it can be found that AES algorithm is most efficient in terms of speed, time, throughput and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. It was concluded that AES algorithm consumes least encryption and HRSA consume longest encryption time. Decryption of AES algorithm is better than other algorithms. When it comes to security, the winner is undoubtedly AES as it is considered unbreakable in practical use. It has been designed in software and hardware and it works quickly and efficiently, even on small devices such as smart phones. With a larger block size and longer keys using a 128 bit block and with 128, 192 and 256 bit keys, respectively, AES will provide more security in the long term.

IV. CONCLUSION

This paper presents a detailed study of the popular Encryption Algorithms such as HRSA, TDES, DSA and AES. The use of internet and network is growing rapidly. So there are more requirements to secure the data transmitted over different networks using different services . AES algorithm can be made much more powerful and secure by increasing the number of iterations in the encryption algorithm to suit the level of security required. demand of application in which going to use security algorithm which factor is important time or security. It must play a fair role between time taken by the algorithm and level of security, both must be reasonable. This application’s main aim is to reduce sever load by showing the minimum response time of each server. This application is very beneficial, powerful, efficient, and user friendly. Future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval and Verification of overall functionality using system Verilog.

REFERENCES

[1] Roy, Rajiv. "Using different encryption techniques for load balancing with cluster-based storage." *IEEE Potentials* 32.2 (2013): 36-39.

[2] Panda, Prabhat K., and Sudipta Chattopadhyay. "A hybrid security algorithm for RSA cryptosystem." *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*. IEEE, 2017.

[3] Mitchell, Chris J. "On the security of 2-key triple DES." *IEEE Transactions on Information Theory* 62.11 (2016): 6260-6267.

[4] Hafsa, Amal, et al. "A hardware-software co-designed AES-ECC cryptosystem." *Advanced Systems and Electric Technologies (IC_ASET), 2017 International Conference on*. IEEE, 2017.

[5] Alam, Shahzad, et al. "Digital image authentication and encryption using digital signature." *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*. IEEE, 2015.

[6] Somani, U., Lakhani, K., & Mundra, M. (2010, October). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In *Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on* (pp. 211-216).

[7] Panda, Prabhat K., and Sudipta Chattopadhyay. "A hybrid security algorithm for RSA cryptosystem." *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*. IEEE, 2017.

[8] Yenuguvanilanka, Jyothi, and Omar Elkeelany. "Performance evaluation of hardware models of Advanced Encryption Standard (AES) algorithm." *Southeastcon, 2008. IEEE*. IEEE, 2008.

[9] Ivanschitz, Bernd-Peter. "Algorithm Selection and Runtime Prediction for the two Dimensional Bin Packing Problem."

[10] Nguyen, Phong Q., and Igor E. Shparlinski. "The Insecurity of the Digital Signature Algorithm with Partially Known Nonces." *Journal of Cryptology* 15.3 (2002).

[11] Jain, Gunjan. "Digital signature algorithm." *International Journal of Innovations in Computing* 1.1 (2012): 1-6.

[12] Khalique, Aqeel, Kuldip Singh, and Sandeep Sood. "Implementation of elliptic curve digital signature algorithm." *International journal of computer applications* 2.2 (2010): 21-27.