International Journal of Science, Technology and Management (IJSTM) **ISSN (online): 2321-774X**
Volume 10, Issue 1, 2023

Analysis of Cryptography Techniques

[1]Bhupender, [2] Ms. Neha

[1]M.Tech. Scholar, [2]Assistant Professor

Department of CSE, BRCM CET, Bahal, Bhiwani, Haryana (India)

[1]bhupender.rangi.51@gmail.com

[2]neha@brcm.edu.in

ABSTRACT-*When it comes to storing, managing & processing data, cloud computing's usage of distant, networked computers housed on the internet has emerged as a game-changing innovation due to its scalability, efficiency & cost-effectiveness. However, it raises concerns about personal information being kept private. This is where cryptography comes in, giving us the means to protect ourselves. Using algorithms & protocols, cryptography in cloud computing safeguards information while in motion and at rest, preserving its privacy, security & accessibility. Encryption & decryption for safe data storage & transmission, key management for restricted access to encrypted data, authentication mechanisms for confirming user identities & cryptographic hash functions for maintaining data integrity are all essential cryptographic techniques in cloud computing. Cryptographic innovations like homomorphic encryption (which enables computation on encrypted data without decryption) & multi-party computation (which enables multiple entities to compute data while maintaining privacy) are gaining traction in the rapidly developing field of cloud security. They might greatly improve cloud storage safety & personal information privacy. While encryption is an important part of secure cloud computing, it is by no means the sole factor to consider. Network protection, access policy & physical security mechanisms should all function in tandem with it. The security infrastructure for cloud computing stands to benefit greatly from future developments in cryptography & its continuing integration with other technologies.*

Keywords: Cryptography, Data Encryption Standard (DES), Advanced Encryption Standard (AES),Cloud Computing, Cloud Security.

INTRODUCTION

Data storage & retrieval have been greatly improved by cloud computing, which provides these services through the internet & makes them scalable, efficient & inexpensive. However, fresh security concerns have emerged alongside these advantages. The provision of cryptographic tools for secure communication, data protection & identity verification in cloud systems is one way in which cryptography contributes to resolving these concerns.

Protecting sensitive information in the cloud requires the use of cryptographic methods & algorithms. This involves:

- Encryption & Decryption: The major means of protecting data privacy is through the use of encryption & decryption. When information is uploaded to the cloud, it is encrypted & only decoded when it is retrieved. This guarantees that the data is unintelligible even if it is intercepted or viewed without permission.
- Key Management: Secure storage & management of encryption keys is crucial to ensuring that only authorized parties have access to [3]sensitive information. Key Management Services (KMS) handle the creation, distribution & destruction of cryptographic keys & are offered by several cloud vendors.
- Authentication & Access Control: Cryptography is also employed in the processes of authenticating people & regulating their access permissions to data. Examples include hashing & storing passwords & using digital signatures to confirm the legitimacy of a server or client.
- Data Integrity: When it comes to protecting sensitive information, cryptographic hash functions are frequently utilized. For each set of input data, they generate a one-of-a-kind character string called a hash. The hash value shifts if the data is modified, suggesting that the data has been altered.
- Secure Communication: Data transmission between the user & the cloud service is encrypted using cryptography. Secure Sockets Layer (SSL) & Transport Layer Security (TLS) are commonly used for this purpose.

More advanced cryptographic techniques are being investigated for use in cloud environments to provide even higher levels of security & privacy. These include Homomorphic Encryption (which permits computation on encrypted data) & Secure Multi-party Computation (which permits multiple parties to compute a function over their inputs while keeping those inputs private).

Remember that encryption is only one part of a comprehensive security plan that also includes physical protection, network security & strong rules & processes for securing cloud data.

There are two main categories of cryptography:

- Symmetric Cryptography: In symmetric cryptography, an encrypted message & its corresponding decrypted one use the same key. When a communication is encrypted, both the sender & the recipient utilize the same key. One type of symmetric cryptography is represented by the Advanced Encryption Standard (AES).
- Asymmetric Cryptography: The two keys used in asymmetric cryptography—the public key, which is freely disseminated & the private key, which is guarded closely—are called "keys." It is the private key that is used to decrypt the[5] encrypted communication, whereas the public [15]key is used to encrypt it. A popular asymmetric cryptography technique is RSA (Rivest-Shamir-Adleman).

Encryption is just one use of cryptography; other applications include digital signatures for verifying an individual's identity, hash functions for checking the consistency of data & cryptographic protocols like SSL/TLS for protecting online transactions.

While cryptography is crucial for online safety, it is still a weapons race between good guys & bad guys. New approaches to crack cryptosystems emerge in tandem with the development of new cryptographic systems. Therefore, the sector keeps developing & changing to meet these new demands.

PROBLEM STATEMENT

Data Encryption Standard (DES):-"DES is a 56-bit key length symmetric block cipher (shared secret key). DES was first released in 1977 as part of the [11]Federal Information Processing Standards (FIPS) 46 standard, however it was deprecated in 2005.
Over 35 years ago, DES encryption was created by the federal government to ensure the confidentiality of all official government communications. The goal was to assure the interoperability of all government systems by adopting a single, secure standard.

The Failure of DES :-

"A series of challenges[11] were sponsored to test how long it would take to decipher a communication, demonstrating [11]that the DES was [18]insufficient & should no longer be utilized in critical systems.[7] Distributed.net & the Electronic Frontier Foundation (EFF) were instrumental in cracking DES.

- It took a brute force assault of 84 days to crack the encrypted message in the DES I competition in 1997.
- Two DES II competitions were held in 1998. It took slightly over a month to solve the first puzzle & the deciphered text read, "The unknown message is: Many hands make light work." The second challenge, which read "It's time for those 128, 192 & 256-bit keys," was completed in under three days.
- In early 1999, the last DES III task was completed in under 22 hours & 15 minutes. The 56-bit DES key was located & the message was decrypted thanks to the combined efforts of the[7] Deep Crack computer (constructed for less than [11]$250,000) at the Electronic Frontier Foundation & the computing network at distributed.net. The phrase "See you in Rome (Second AES Candidate Conference, March 22-23, 1999)" was decoded after searching through only 30% of the key space, demonstrating definitively that DES is now obsolete.

The Failure of 3DES :-

Using DES encryption three times is known as Triple DES (3DES) or Triple Data Encryption Algorithm (TDEA). However, brute-force[18] assaults have been shown to be able to crack even Triple DES (which also has the downside of being significantly slower).

On July 19, 2018, NIST released draft retirement recommendations for TDEA/3DES. According to the recommendations, Triple DES should be phased out for all new uses after 2023"[11]

Advanced Encryption Standard (AES):-

The 2001 [11] publication of the FIPS 197 standard. The flexibility to use keys[18] of varying lengths is the primary strength of AES data encryption, despite the algorithm's higher mathematical efficiency & elegance. Since AES lets you pick between [11] a key size of 128 bits, 192 bits, or 256 bits, it is exponentially more secure than DES's 56-bit key.

The Feistel network is used structurally in DES to split the block in half before it undergoes the encryption process. of contrast, the encrypted block of AES is created by a sequence of substitution & permutation stages, known as permutation-substitution. Although the [18]creators of the DES algorithm should be commended for their work, the AES algorithm is the culmination of far more work by cryptographers as a whole.

The National Institute [11]of Standards and Technology (NIST) mandated that the DES replacement algorithm be effective in both software & hardware implementations. (Initially, only hardware implementations of DES were viable.) The algorithms' speeds were analyzed using reference implementations written in Java and C. AES was selected after a [8]massive investment of time & money into a global competition that involved 15 other proposals & as many research teams"[18].

Rijndael was chosen as the proposed[16] Advanced Encryption Standard (AES) in October 2000, according to a press statement from the National Institute of Standards and Technology (NIST).

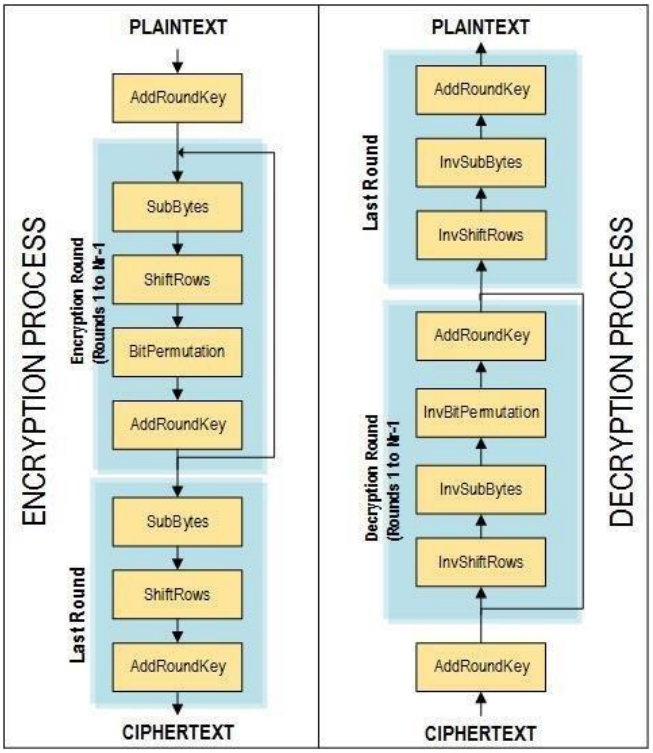

Figure 1:AES Structure

PREVIOUS IMPLEMENTATION

"It was widely known that the Data Encryption Standard (DES) could be easily broken using cryptanalysis or brute force. There were alternatives to DES that might be used for cryptographic purposes, but many of them were either deemed proprietary or protected by patents. It's not too difficult to try all 256 potential keys these days. A DES password breaker that costs 25,000 & works in a few hours may be built. Only 56 bits can be used in DES. Both the integrity & secrecy of a system are compromised when a nonce is reused. In the case of short tags, it is quite simple to manufacture message forgeries if the same nonce[12] is used twice by an adversary. For example, if[9] the tag length is 32 bits, a forged cipher text can be generated after 216 forging attempts & 216 encryptions of selected plaintexts (also of length 216). When enough examples of forgeries exist, creating new ones is as quick as printing a new one. The fact that both DES[12]& AES rely on a 64-bit block size is a disadvantage. Key length can be increased to 1024 bits if a bigger block size is desired for efficiency & security reasons"[17].

PROPOSED MODEL

- AES Implementation:-

"In order to implement its circular structure, the [12]AES-1024 algorithm makes advantage of the transformation described in the preceding section. [12]First, 128-bit data undergoes a byte substitution & then depending on the row number, a 0-7 left rotation is done. In the Mix Column transformation, the columns are multiplied by the newly created matrix column by column.

The 1024 bits of input plaintext are structured as an array of 128 bytes, with values produced through replacement boxes being used in their place. According[14] to the concepts of diffusion-confusion laid out by Shannon for designing cryptographic algorithms, this is done to increase safety.

Shift Row transformation involves moving the rows of the resultant matrix after the[14] initial 1024 bits are replaced with values from the S-boxes. In this step, the [12]bytes in each row of the input data matrix will be rotated by 90 degrees to the left. The row number can be used to infer the variation in the number of left rotations across rows.

The AddRoundKey operation is carried out to increase the complexity of the key-ciphertext interaction & to adhere to the confusion principle. The resultant data matrix from the previous step is used in this step's addition operation, which is a bitwise XOR with the round's subkey (an addition operation in GF (2n)). It's[14] important to note that the round key is [17]1024 bits long & is laid out in a square matrix with eight columns, each of which contains 16 bytes[17].

The new AES-1024 method uses a 1024-bit input key to produce 10 sub-keys, one for each of the 10 AES rounds. The input key of 512 bits is expanded into eight words of eight bytes each during the round keys operation".[17]

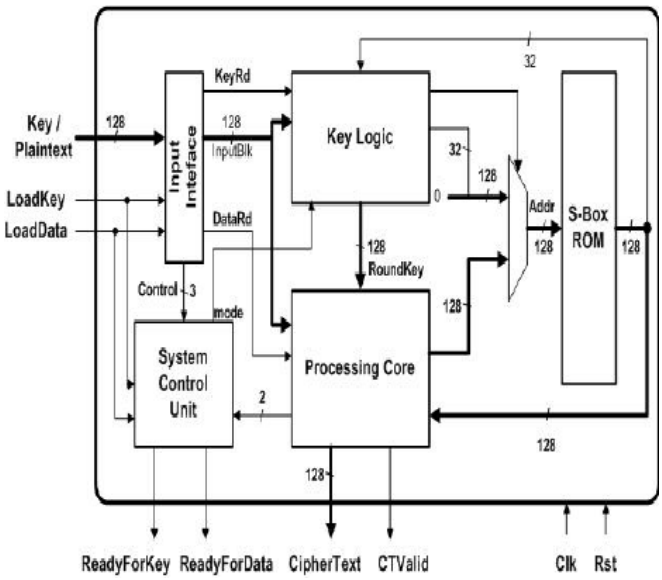

Figure 2: Block diagram of AES Core

- DES Implementation:-

DES uses the ciphering methods of randomness & noise dispersion to secure data. Substitution creates muddled thinking. Parts of the original data are replaced with new data that has been carefully selected. Based on the [12]key

and the original plaintext, a replacement value is selected. Permutation is the[14] means through which diffusion is performed. The information is mixed up by switching around the order of the different subsections. Both the key & the original plaintext serve as the basis for these variations.

The DES algorithm dictates the nature of the replacements & permutations to be used. Mathematical operations are performed on subsets of [14]the key & the data & the results are fed into a look-up table. In DES, the tables used for substitution & permutation are referred to as S-boxes and P-boxes, respectively. These lookup tables are implemented in software as arrays, with the input key or data serving as the array's index. The S-boxes & P-boxes are often integrated such that each round's substitution & subsequent permutation may be looked up using a single look-up.

Data Encryption [13] Standard (DES) is implemented using an algorithm known as Data[13] Encryption Algorithm (DEA), which takes the right 512 bits of a 1024-bit input[12] data block & expands them into a 48-bit[12] block. These are the "expansion permutation steps" in the jargon.
DES can decrypt plain text blocks as large as 1024 bits. The key is 128 bits in length,[14] making it more secure. The 1024-bit input plain[17] text block is split into four plain text chunks, P1–P4, with each chunk being 16 bits in size. As there are 8 iterations of the method, P1 through P4 are inputs in the first round. The results of the first round are fed into the second. The results of the second round are fed into the third & so on. Six new keys are created from the original key in each round. There are 16 bits in each of the subkeys. We'll use keys 1–6 (K1–6) for the initial round. Keys K7 through K12 will be used in the next round. The eighth & final round will use keys K43–K48. The last stage is an output transformation that requires only four auxiliary keys (K49–K52). The output transformation results in four blocks of cipher text, C1 through C4, which serve as the final output. Together, they make up the 64-bit cipher text block. The addition & multiplication in this method are performed modulo 216 & modulo 216+1, respectively. This makes use of key shifting as a method.

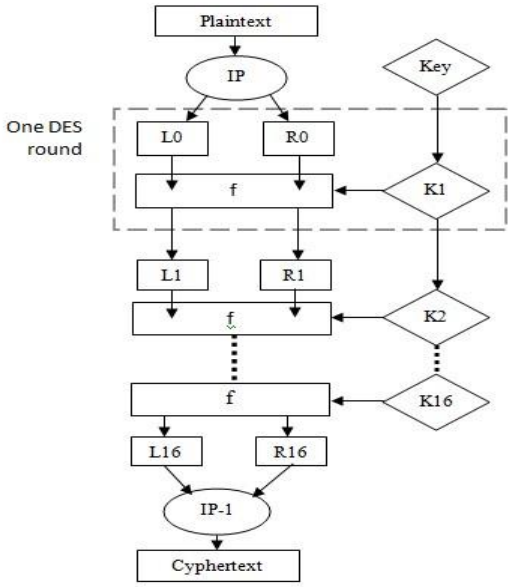

Figure 3: Block diagram of DES Core

This plan of this show employments the AES & DES calculations together. Figure 4 appears how records are scrambled when put away within the cloud. 128-bit AES encryption is connected to records at whatever point they are made & spared. The record to begin with goes through the [Include Circular] key, at that point 10 rounds of sub-bytes, at that point [Move Lines], at that point [Rearrange Columns], then [Add Round] key. This can be taken after by a last circular of sub-bytes, taken after by "move line" & "include circular key".

Figure 4:Record Encryption & Creation of signature when giving Cloud Capacity

Once the record has gone through all these forms, it is alloted the message process work "SH1", coming about in a process. The process is changed over to a DES signature employing a 1024-bit private key. A open key is created utilizing the private key some time recently the encryption handle starts.

When the recipient/client opens the record for signature confirmation, 1024-bit marks are utilized. Utilize the message digest work "SHA1" to make the process. The signature & record are unscrambled by combining with the open key made amid encryption to make the anticipated process here. The process is compared with the anticipated process to see in case the keenness of the climate record has been compromised. In the event that both cruel the same, record keenness isn't compromised. In the event that they don't coordinate, the file has been altered & isn't steady. This handle is appeared in Figure 5. A message process "SHA1" could be a cryptographic hash work comprising of a grouping of numbers shaped from a one-way hash. The result produced by SHA-1 is a message process consisting of 20 bytes, or 160 bits. The SHA-1 hash consists of 40 characters in total.

Figure 5: Decrypting AES files during recovery & scanning file contents with DSA

RESULTS

"The Data Encryption Standard algorithm & Advanced Encryption Algorithm is implemented[14] using NS2 simulator"[12].

Figure 6: Performances of DES & AES

Key Size	AES	DES
64	2400	1800
128	2550	1600
196	2300	1700
256	2500	1800
512	2600	1900
1024	2400	2000

Table 1:Performance of AES & DES

Security:-Because of the many cryptographic threats, it is important to consider the security properties of each method. The speed with which the method can encrypt & decode data blocks of varying sizes depends on the value set here.

Figure 7: Security of AES Vs DES

Key Size	AES	DES
32	400	400
64	1200	260
128	1420	600
196	1400	800
256	1600	950
512	2100	1100
1024	2550	1600

Table 2: Security Comparison of AES Vs DES

CONCLUSION

"Since encryption methods are crucial to ensuring the confidentiality of transmitted data, it is imperative that new, more robust cryptographic algorithms be devised & put into use. A new variant of AES & DES (1024) has been developed, which uses a 1024-bit input [12]block& a 1024-bit key size rather than the 128-bit used by the original algorithms. The whole plan for using the new tool was also shown. The length of a key makes a significant difference in how long it takes a brute-force computer to crack the AES algorithm. The simulation[12] results for different key sizes for AES take into account the five different key sizes that are feasible, namely 128 bits, 192 bits,[12] 256 bits, 512 bits & 1024 bits. There is a noticeable shift in the number of key rounds & the amount of time needed due to its increased key size. The algorithm has a wide range of platforms & applications where it may be safely & efficiently deployed. When contrasting the outcomes of each implementation, Increases in both key size & input block size improve the algorithm's security & performance, respectively. The suggested algorithm's increased space requirements make it well-suited for use in contexts requiring both a high level of security & a high throughput. The algorithms' efficiency was measured using a variety of criteria. It is demonstrated that both techniques have distinct time requirements on various computers. Time required for the same method over the same data packet on various devices varies. The provided results demonstrated that AES is more secure than DES, particularly when subjected to a brute-force assault"[12].

REFERENCES

[1] M.E. Hellman, "DES will be totally Insecure within Ten Years", lEEE Spectrum, Vo1.16, N0.7, pp32 39, July 1979.
[2] Alani, M.M., "A DES96 - Improved DES Security", 7th International Multi-Conference on Systems, Signals and Devices, Amman, 27-30 June 2010.
[3] Manikandan. G, Rajendiran. P, Chakarapani. K, Krishnan. G, Sundarganesh. G, "A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.
[4] Shah Kruti R., BhavikaGambhava, "New Approach of Data Encryption Standard Algorithm", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[5] A. Nadeem, "A Performance Comparison of Data Encryption Algorithms", IEEE Information and Communication Technologies, pp.84-89, 2006.
[6] Sannbansahmoud, WilliamElamary and shadiAdudalifa, " Enhanecement the Security Against Modern Attacks by Using Variable Key Block Cipher", International Arab Journal of – e- technologies, Vol 3, No:1, 2013.
[7] AviKak"AES: The Advanced Encryption Standard Lecture Notes on "Computer and Network Security"May 1, 2015.
[8] Sumitra, "Comparative Analysis of AES and DES Security Alogrithm", International Journal of Scientific and Research Publications, Vol3, Issue 1, January 2013.
[9] Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopad3, Someshwar Vaidy4, Mahesh Sana, " AES Algorithm using 512 Bit Key Implementation for Secure Communication", International journal of innovative Research in Computer and Communication Engineering, Vol. 2 Issue 3, March 2014.
[10] Nikolas Bardis, Konstantinos Ntaikos, "Design of a Secure Chat Application based On AES Cryptographic Algorithm and Key Management", JIRETVol.3, no. 2, 2011.
[11] https://www.precisely.com/blog/data-security/aes-vs-des-encryption-standard-3des-tdea
[12] https://shanlaxjournals.in/journals/

[13]Alen Salkanovic, Sandi Ljubic, Ljubisa Stankovic, Jonatan Lerga. "Analysis of Cryptography Algorithms Implemented in Android Mobile Application" , Information Technology and Control, 2021
[14] ENHANCING DES AND AES WITH 1024 BITS KEY Ms. Ramya G.,Ms. Anita Madona M., International Research Journal of Engineering and Technology (IRJET),Volume: 02 Issue: 04, July-2015
[15] "Computational Intelligence, Communications, and Business Analytics" , Springer Science and Business Media LLC, 2017
[16] Kadri, Akeem Femi. "Enhancement of Advanced Encryption Standard Performance on Hidden Data Using Residue Number System" ,Kwara State University (Nigeria), 2023
[17] https://www.irjet.net/
[18] https://www.ecu.edu.au/research/overview\