Research Article

A HYBRID CRYPTOGRAPHIC FRAMEWORK FOR SECURING CLOUD DATA USING BLOWFISH AND HOMOMORPHIC ALGORITHMS

Ushadevi R., Viswanathan M.
Department of Computer Science, Sri Krishnasamy Arts and Science College, Sattur

ABSTRACT

With the rapid expansion of internet-based applications, ensuring robust data security has become a critical concern—especially in cloud environments where data centers are globally distributed. Cryptographic techniques, both symmetric and asymmetric, play a pivotal role in safeguarding sensitive information. Among these, strong user authentication mechanisms are essential to prevent unauthorized access. This paper explores the significance of data protection in cloud computing and evaluates various encryption and authentication strategies, with a focus on Blowfish and Homomorphic encryption algorithms.

Keywords: Cloud Computing, Data Security, Blowfish Algorithm, Homomorphic Encryption, Cryptography

INTRODUCTION

Cloud computing refers to a network of distributed servers and data centers that deliver on-demand services via the internet. These services are not hosted locally on the user's device but are accessed remotely, offering flexibility and scalability. Users benefit from reduced infrastructure costs and the ability to store and retrieve data from any location. However, this convenience introduces security challenges, as users entrust their data to third-party platforms. Ensuring confidentiality, integrity, and availability becomes paramount. Cryptographic methods are employed to maintain these security principles, particularly in cloud-based environments [1]. Security becomes big issue when anybody stores its important information to a platform which isn't directly controlled by the user and which is way away. While sending of knowledge and through storage data is under threat because any unauthorised user can access it, modify it, so there's got to secure data. a knowledge is secure, if it fulfils three conditions (i) Confidentiality (ii) Integrity (iii) Availability. Confidentiality means the info is understandable to the receiver just for all others it might be waste; it helps in preventing the unauthorised disclosure of sensitive information. Integrity means data received by receiver should be within the same form, the sender sends it; integrity helps in preventing modification from unauthorized user. Availability refers to assurance that user has access to data anytime and to any network. within the cloud confidentiality is obtained by cryptography [7].

SECURITY ISSUES OF CLOUD COMPUTING

The interconnected nature of cloud networks exposes data to various threats, including unauthorized access, data tampering, and privacy breaches. Key concerns include

maintaining data integrity, ensuring availability, protecting confidentiality, and preserving transparency and control over data location. Security can be reinforced through access control mechanisms and encryption protocols. Both service providers and clients share responsibility for implementing and verifying robust security measures [6].

PROBLEMSTATEMENT

Cloud computing faces numerous challenges—ranging from privacy and data segregation to accountability and secure storage. Among these, data security stands out as the most pressing issue. Different user groups, such as academic institutions and enterprises, have distinct security expectations. For academic users, security must be balanced with performance, while enterprises demand stringent protection for sensitive business data. This paper focuses on enhancing data security in cloud computing environments [5].

EXISTING ALGORITHMS

Many organisations and other people store their important data on cloud and data is additionally accessed by many persons, so it's vital to secure the info from intruders. to supply security to cloud many algorithms are designed. Some popular algorithms are: -

Data Encryption Standard (DES)

This stands for encoding Standard and it had been developed in 1977. it had been the primary encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES consists of 64 bits key size with 64 bits block size. Since that point, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher [8].

Algorithm: Function DES_Encrypt (M, K) where M = (L, R)
M->IP (M)
For round 1 to 16 do
K->SK (K, round) L->L xor F(R,Ki) swap(L, R) end swap (L, R) M->IP-1(M) return M End

Advance Encryption Algorithm (AES)

(Advanced Encryption Standard), is that the new encryption standard recommended by NIST to exchange DES. Brute force attack is that the only effective attack known against it, during which the attacker tries to check all the characters' combinations to unlock the encryption. Both AES and DES are block ciphers. it's variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round counting on the key size. AES Encryption is fast and flexible; it is often implemented on various platforms especially in small devices. Also, AES has been carefully tested for several security applications [8].

Triple- DES (TDES)

This was developed in 1998 as a brief of DES. during this standard the encryption method is analogous to the one in original DES but applied 3 times to extend the encryption level. But it's a known incontrovertible fact that 3DES is slower than other block cipher methods. this is often an enhancement of DES and it's 64-bit block size with 192 bits' key size. 3DES has low performance in terms of power consumption and throughput in comparison with DES. It requires always longer than DES due to its triple phase encryption characteristics [8].

Algorithm:

For j = 1 to three { Cj,0= IVj
For i = 1 to nj

{
Cji = EKEY3(DKEY2 (EKEY1 (Pj, iCj, i-1))) Output Cj, i
}
}

Diffie- Hellman Key Exchange

Diffie–Hellman key exchange may be a specific method of exchanging cryptographic keys. it's one among the earliest practical samples of key exchange implemented within the sector of cryptography.

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be wont to encrypt subsequent communication employing a symmetric key cipher [2].

IDEA

International encoding Algorithm was proposed by James Massey and Xuejia Lai in 1991.It is considered as best symmetric key algorithm. It can take 64 bits of plain text with a key size of 128 bits. IDEA consists of 8.5 rounds. All rounds are similar except the one. In IDEA the 64 bits of knowledge is split into 4 blocks each having size 16 bits. arithmetic operators are also applied in sub blocks. There are eight and half rounds in IDEA each round contains different sub keys. 52 keys were used to perform different rounds. In round 1 the K1 to K6 sub keys are generated, the sub key K1 has the primary 16 bits of the first key and K2 has subsequent 16 bits similarly for K3, K4, K5 and K6 [3]. Therefore, for round 1 (16*6=96) 96 bits of original cipher key's used. what's the sequence of operations performed in each round? Let I1, I2 …I6 be the inputs to round 1, functions in round 1 are:

- (i) Multiply I1 and K1.

Add I2 and K2.

Add I3 and K3.

Multiply I4 and K4.

Now, step 1 is EXOR with step 3.

Step 2 EXOR with step 4.

Multiply step 5 with K5.

Similar operations are performed in other rounds.

PROPOSED ALGORITHMS

Homomorphic Encryption

Homomorphic encryption uses asymmetric key algorithm during which two different keys are used for encryption and decryption i.e. public key and personal key [10]. In mathematics homomorphic means conversion of 1 data set to a different, without losing its relation between them. In homomorphic complex mathematics functions are applied to encrypt the info and similar but reverse operation is applied to decrypt the info [4].

RSA

This is an online encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is that the most ordinarily used encryption. Till now it's the sole algorithm used for personal and public key generation and encryption. it's a quick encryption [5,8].

Algorithm

Key Generation: KeyGen(p, q)

Input: Two large primes –p, q Compute n = p.q $\varphi(n) = (p-1)(q-1)$

Choose e such $\gcd(e, \varphi(n)) = 1$ Determine d such $e.d \equiv 1 \bmod \varphi(n)$ Key: Public key = (e, n) Secret key= (d, n)

Encryption: $c = m^e \bmod n$

where c is that the cipher text and m is that the plain text.

RSA features a multiplicative homomorphic property i.e., it's possible to seek out the merchandise of the plain text by multiplying the cipher texts. The results of the operation are going to be the cipher text of the merchandise. Given ci = E (mi) = mie mod n, then (c1. c2) mod n = (m1. m2) e mod n

Blowfish Algorithm

This was developed in 1993. it's one among the foremost common public algorithms provided by Bruce

Schneier. Blowfish may be a variable length key, 64-bit block cipher. No attack is understood to achieve success against this. Various experiments and research analysis proved the prevalence of Blowfish algorithm over other algorithms in terms of the time interval. Blowfish is that the better than other algorithms in throughput and power consumption.

Algorithm:

Divide x into two 32-bit halves: xL , xR For i = 1to 16:

xL = xL XOR Pi xR = F(xL) XORxR

Swap xL andxR

Next i Swap xL and xR (undo the last swap)

xR = xR XOR P17

xL = xL XOR P18

Recombine xR and xL

CONCLUSION

Cloud computing has revolutionized data storage and access, offering scalable solutions for individuals and organizations. However, the reliance on remote servers necessitates robust security protocols. While traditional algorithms like DES and AES provide foundational protection, emerging techniques such as Homomorphic encryption and Blowfish offer enhanced security features. Strengthening these algorithms is essential to address evolving threats and ensure data integrity in cloud environments.

FUTURE SCOPE

As cloud adoption continues to grow, so does the need for advanced security mechanisms. Virtualization and remote access are key benefits, but they must be supported by reliable encryption and authentication systems. Future research should focus on developing resilient algorithms that can withstand sophisticated attacks and adapt to dynamic cloud architectures.

REFERENCES

1. Alexa Huth and James Cebula ‘The Basics of Cloud Computing’, United States Computer Emergency Readiness Team. (2011).

2. Ch. Chakradhara Rao and A.V.Ramana,”Data Security in Cloud Computing”, International Journal of Current Trends in Engineering and Research.

3. Qi. Zhang •Lu. Cheng, RaoufBoutaba, “Cloud computing: state-Of-the-art and research Challenges”, “The Brazilian Computer Society”, April 2010.

4. Anca apostu, Florina puican, Geanina ularu, George suciu, Gyorgy todoran, “Study on advantages and disadvantages of Cloud Computing –the advantages of Telemetry Applications in the Cloud”, Recent Advances in Applied Computer Science and Digital Service.

5. L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.

6. *A Fully Homomorphic Encryption*

Scheme, (2009), C. Gentry.

7. Sandro Rafaeli, "Survey of key management for secure communication", ACM Computing Surveys, 2013

8. Gurpreet Singh, SupriyaKinger "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.