IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

USE OF DIGITAL SIGNATURE WITH DIFFIE HELLMAN KEY EXCHANGE AND AES ENCRYPTION ALGORITHM TO ENHANCE DATA SECURITY IN CLOUD COMPUTING

[1.]PRANIT RAJ CHITRAPU [2.]KAVALA BHASKARA DURGA [3.]NAINAPATRUNI JAYANTH
[4.]CHITTI KISHORE [5.]NALLA KISHOR [6.]G.VENKATA RAMANA
Under the guidance of **K.PRASANNA LATHA**
Assistant Professor
Department of Computer Science and Engineering,
Visakha Institute of Engineering and Technology
Visakhapatnam

ABSTRACT: Cloud technology emerges as the cornerstone of the upcoming decade, offering users the ability to store vast amounts of data remotely and access it from any location, using diverse terminal devices as needed. However, challenges such as privacy, data protection, secrecy, authentication, and access control persist in cloud computing. To address these issues, researchers employ a variety of encryption techniques and mechanisms to bolster security. By integrating encryption algorithms with authentication techniques and key exchange protocols, a three-way mechanism is established, safeguarding authentication, data security, and verification simultaneously. This study proposes the utilization of the Advanced Encryption Standard (AES) encryption method in tandem with digital signatures and Diffie-Hellman key exchange to ensure the confidentiality of cloud-stored data. The integration of these methods ensures robust protection against potential threats. Should the key in transit be compromised, the Diffie-Hellman key exchange mechanism remains resilient, as the key's meaninglessness without the user's private key renders it ineffective to unauthorized parties. This three-way approach forms a formidable barrier against hacking attempts, enhancing the security of cloud-based data.

1. INTRODUCTION

Cloud computing offers a flexible and cost-effective way for businesses to access technology resources. Imagine it as renting computing power over the internet, instead of having to buy and maintain your own servers and software. This on-demand service allows companies to scale their resources up or down as needed, so they only pay for what they use.

There are different cloud service models available, like SaaS (Software as a Service) which provides access to applications like Gmail, PaaS (Platform as a Service) that lets developers build custom applications, and IaaS (Infrastructure as a Service) that offers access to storage and computing power.

While cloud computing offers significant benefits, security is a major concern. Since data is stored and accessed remotely, there's a risk of unauthorized access. Encryption helps mitigate this risk by scrambling data into an unreadable format, but it can be computationally expensive to implement for large datasets.

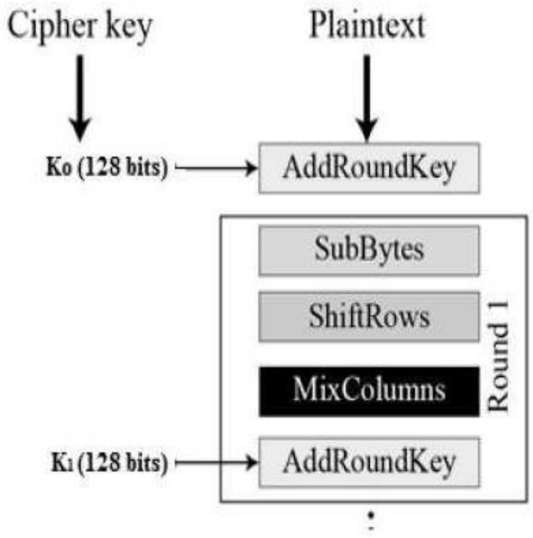

Fig: Encryption process

1. LITERATURE REVIEW

The significance of implementing digital signatures with the RSA encryption algorithm to enhance data security in cloud computing environments. It emphasizes the transformative impact of cloud computing, offering dynamic resource allocation, scalability, and cost-effectiveness over the internet. Security emerges as a critical concern, with cloud networking architectures facing significant challenges despite their numerous advantages, including reduced capital expenditures and enhanced scalability across service models like SaaS, PaaS, and IaaS.

Privacy and security issues persist as barriers to cloud adoption, particularly for sensitive data and applications. To address these concerns, multidimensional cloud computing data security models are proposed, focusing on user authentication, data encryption, and rapid data regeneration mechanisms. Additionally, modern encryption techniques play a crucial role in ensuring data security, with various algorithms evaluated for their effectiveness and performance in cloud computing environments.

Furthermore, the review underscores the uncertainty surrounding cloud computing security, emphasizing the need for comprehensive examinations and solutions. It identifies new aspects introduced by the cloud model, such as multi-tenancy and elasticity, which contribute to the complexity of security challenges. Comprehensive analyses of cloud architecture, features, stakeholders, and service delivery methods are essential for developing effective security solutions.

2. IMPLEMENTATION

Cloud computing allows data and services to be utilized and stored anywhere that is not under the direct control of an organization. This facility raised issues related to integrity, privacy, secrecy, and other security, which made a secure computer environment necessary. To foster confidence in computing and maintain data confidentiality, a system that verifies, authenticates, and encrypts data is required.

Our proposed design employs protective measures in three distinct ways. Firstly, keys for the exchange stage are generated via the Diffie-Hellman method. User authentication is achieved through digital signatures, followed by AES encryption to safeguard user data files. These measures collectively establish a secure computing environment, preventing data tampering at the server end. Furthermore, we employ a trusted computing platform to encrypt user data files and utilize a dedicated storage server for their safekeeping.

To upload a file to the cloud server, a user must first log in and perform a Diffie-Hellman key exchange for key generation. Subsequently, their digital signature is verified. Upon AES encryption of the user's data file, it is then securely transferred to another cloud storage server. When a client requires the same file, retrieval is facilitated from the cloud server. This process entails the user logging in, exchanging encryption keys, selecting the desired file for download, authenticating via digital signature, and ultimately decrypting the stored file using AES.

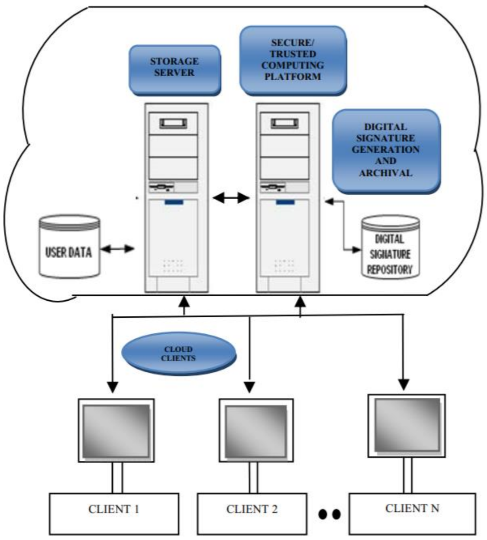
STORAGE SERVER
SECURE/ TRUSTED COMPUTING PLATFORM
DIGITAL SIGNATURE GENERATION AND ARCHIVAL
USER DATA
DIGITAL SIGNATURE REPOSITORY
CLOUD CLIENTS
CLIENT 1
CLIENT 2
CLIENT N

Fig: System architecture

4. ALGORITHMS

DIFFIE-HELLMAN ALGORITHM:

A shared secret for confidential communications across a public network is created by the Diffie-Hellman method, which uses the elliptic curve to produce points and the parameters to derive the secret key. The procedure involves four variables: two private values (A and B), a primitive root (G), and a prime (P). The numbers P and G are available to the public in both situations. After selecting two private values—let's use Alice and Bob as an example—each user creates a unique key, which they then share with the other user or users. After obtaining the key, the other person creates a secret key, giving them the identical secret key to encrypt with.

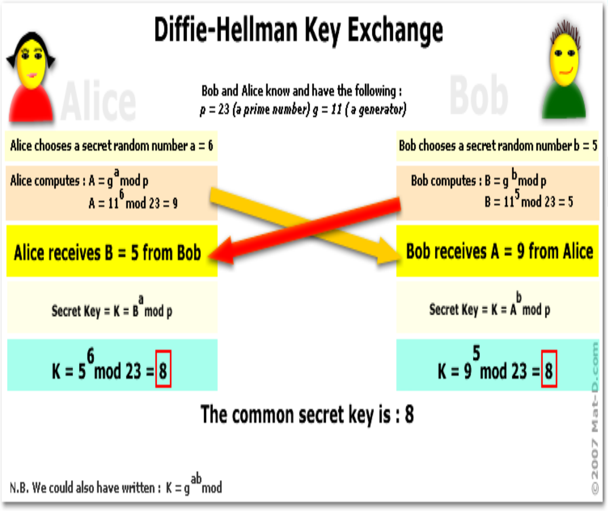
Diffie-Hellman Key Exchange
Alice
Bob
Bob and Alice know and have the following :
p = 23 (a prime number) g = 11 (a generator)
Alice chooses a secret random number a = 6
Bob chooses a secret random number b = 5
Alice computes : A = g^a mod p
A = 11^6 mod 23 = 9
Bob computes : B = g^b mod p
B = 11^5 mod 23 = 5
Alice receives B = 5 from Bob
Bob receives A = 9 from Alice
Secret Key = K = B^a mod p
Secret Key = K = A^b mod p
K = 5^6 mod 23 = 8
K = 9^5 mod 23 = 8
The common secret key is : 8
N.B. We could also have written : K = g^ab mod
©2007 Mat-D.com

Fig: Diffie hellman key exchange

ADVANCED ENCRYPTION STANDARD (AES):

The Advanced Encryption Standard (AES) is currently the most widely used symmetric encryption method (AES). It is found to be at least six times faster than triple DES. Since DES was growing less secure, its key size needs to be increased. The increased computer capability was considered to make it susceptible to an exhaustive key search assault. To circumvent this issue, the Triple DES algorithm was developed.

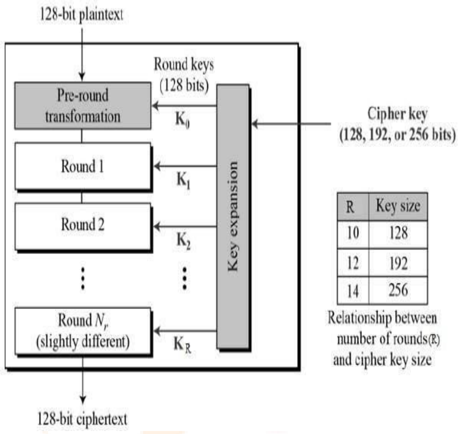

Fig: AES structure

In contemporary encryption, AES is extensively utilized and supported in both hardware and software. As of right now, no practical cryptanalytic attack against the AES algorithm has been discovered. AES has an inherent characteristic that allows it to combat future advancements in the capacity to perform exhaustive key searches: the flexibility to modify the length of its keys. AES security depends on proper implementation, just as DES security depends on superior key management.

5. CONCLUSION

In this study, we propose to secure cloud data privacy by utilizing the Advanced Encryption Standard (AES) encryption technique in combination with digital signatures and Diffie Hellman key exchange. Even if a key in transit is compromised, the Diffie Hellman exchange facility—which requires the private key of an authentic user to decode it—will remain worthless, regardless of how well-known it is. A three-way approach that is hard for hackers to crack has been developed to secure cloud-based data.

6. REFERENCES

1. Secure Cloud Data Using Attribute Based Encryption, International Research Journal of Engineering And Technology(IRJET) An issue to the date 04-Apr 2019.

2. Use Of Digital Signature with Diffie Hellman Key Exchange and Hybrid Cryptography algorithm to Enhance Data Security in Cloud Computing. International Journal of Scientific and Research Publications, volume 5, Issue 6-June 2015.

3. Data Security in Cloud Computing, Fifth International Conference on Future Generation Communication Technologies (FGCT 2016)

4. Data Security Approach in Cloud computing using SHA , International Research Journal of Engineering and Technology (IRJET) Issue to the date 06-june-2017.

5. Single to Multi Cloud Data Security in Cloud Computing (IRJET) issue date 03-mar-2019

6. Data Security Methods in Cloud Computing , Livia Maria BRUMA Economic Informatics Doctoral School , issue date 2020

7. Security Measures in Cloud Computing (IRJET) ISSUE DATE 04-APR-2021.

8. Advanced Security Using Encryption, Compression And Stenography Techniques, (IRJET) issue date 06-june-2023.