RESEARCH ARTICLE OPEN ACCESS

Secure Data with Key Managers by Using Shamir Scheme and AES Algorithm

Prof S. Athinarayanan [1], S. Nivetha Priya [2], R. Supriya [3]
Professor [1], Student [2] & [3]
Department Of Information Technology
Prathyusha Engineering College, Chennai
Tamil Nadu – India

ABSTRACT

Network security consists of policies and practices used to prevent and monitor unauthorized access, misuse, modification or denial of a network. The intent of a risk analysis is to identify the components of the network, evaluate the importance of each component, and then apply an appropriate level of security. Network security consists of both public and private, that are used in everyday jobs .Normally any environment is used to store data and encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a security key or password that enables to decrypt. Here two algorithms are used, (a) Shamir's (k , n) threshold scheme and (b) AES (Advanced Encryption Standard) Algorithm Shamir's (k , n) threshold scheme is used for the management of keys that uses K shares out of n to rebuild the key during decryption. AES Algorithm is used for Encryption and Decryption process. This Algorithm makes the system more dependable against hacking and failure of one of the key managers. According to the length of the key the security will be more stronger. Our proposed system provides better solution to user who needs maintenance of data by securely.

Keywords: - AES, Chiper

I. INTRODUCTION

Network security is a big topic and is growing into a high profile (and often highly paid) Information Technology (IT) specialty area. Security-related websites are tremendously popular with savvy Internet users. The popularity of security-related certifications has expanded. Esoteric security measures like biometric identification and authentication – formerly the province of science fiction writers and perhaps a few ultra-secretive government agencies. Yet, with all this focus on security, many organizations still implement security measures in an almost haphazard way, with no well-thought-out plan for making all the parts fit together. Computer security involves many aspects, from protection of the physical equipment to protection of the electronic bits and bytes that make up the information that

Representing system characteristics and capabilities as utility, causes the user to focus on aspects directly related to data (security, transmission, processing). by certain vendors requires high level of trust and security Data being the principal asset for organizations

To avoid unauthorized access to data, access control mechanism must be enforced. Moreover, data leakage and data privacy strategies must be employed so that only authorized users can access and utilize data. Encryption techniques provide a sensure privacy and confidentiality of stored data.

Security Terminology

Attack

In the context of computer/network security, an attack is an attempt to access resources on a computer or a network without authorization, or to bypass security measures that are in place.

Audit

To track security-related events, such as logging onto the system or network, accessing objects, or exercising user/group rights or privileges.

Breach

Successfully defeating security measures to gain access to data or resources without authorization, or to make data or resources available to unauthorized persons, or to delete or alter computer files.

Brute force attack

Attempt to "crack" passwords by sequentially trying all possible combinations of characters until the right combination works to allow access.

Protecting the Servers

File servers on which sensitive data is stored and infrastructure servers that provide mission critical services such as logon authentication and access control should be placed in a highly secure location. At the minimum, servers should be in a locked room where only those who need to work directly with the servers have access. Keys should be distributed sparingly, and records should be kept of issuance and return. If security needs are high due to the nature of the business or the nature of the data, access to the server room may be controlled by magnetic card, electronic locks requiring entry of a numerical code, or even biometric access control devices such as fingerprint or retinal scanners. Other security measures include monitor detectors or other alarm systems, activated during non-business hours, and security cameras. A security guard or company should monitor these devices.

II. EXISTING SYSTEM

The FADE is a light-weight and scalable technique that assures the deletion of files from cloud when requested by the user. However, during our analysis, FADE fell short on issues of security of keys and authentication of participating parties. In this existing process there is a man-in-the-middle (intruder) between client and KM. The intruder can intercept user policy and send modified policy to KM. Now client didn't receive appropriate key from KM, this compromise may lead to the loss of data. Here we used single key server, so the data security issue may occur. Diffie-Hellman algorithm is used to provide Data Security.

III. DISADVANTAGES

- If the key is once lost then the data also lost and may data should be misused or hacked.
- The long term continuous assurance of their data safety is the challenging task.
- Because of using the single key server the data may be easy to hack or misuse.
- Man in the middle attack, key management becomes a prime issue in the case of decryption.

IV. PROPOSED SYSTEM

First the Data which is encrypted with the secret key by using standard encryption algorithm. Second the key is splitted into multiple key managers.Each and every splitted key is encrypted and stored. Now as the result of encryption the data should be in the form of modified data(cipher text).In which Shamir's (k,n) Threshold Scheme is used for the management of keys that uses k shares out of n to rebuild the key. Advanced Encryption Standard(AES) is a cryptographic Symmetric block cipher algorithm use same key for encryption and decryption process.

ADVANTAGES:

- If one key is lost then other keys are used to recover the original key.
- It is difficult to hack the data storage in cloud by using multiple key managers.
- In which Shamir's(K,N) threshold scheme is used for the management of keys.
- A single point of failure should not affect the availability of data.

ARCHITECTURE:

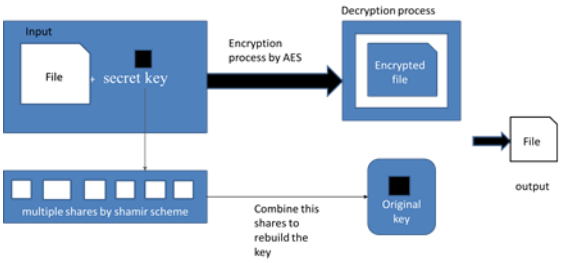


Fig 4 Architecture

V. MODULE DESCRIPTION

KEY GENERATION AND ENCRYPTION PROCESS:

Encryption is the process of transforming information (called plaintext) into an Standard) algorithm. The secret key used in the encryption, it

is the same key going to use in decryption also. Key Generation and encryption process. Here the length of the key is 128 bit.

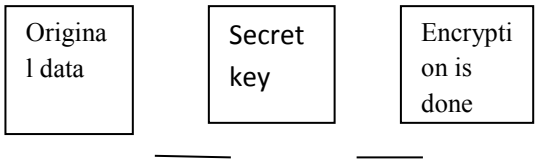


Fig5.1 key generation and encryption process

5.2 KEY SPLITTING ANALYSIS:

The shamir's threshold scheme is used for the management of keys that uses K shares out of n to rebuild the key during decryption. Here the original key is splitted into multiple key managers. If one key is lost other keys are used to recover the secret key. Using multiple key managers the availability of data does not affected.

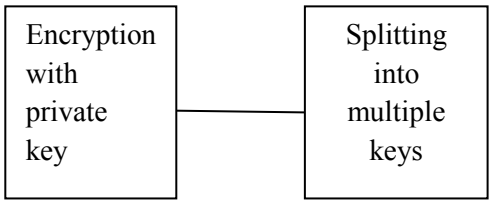


Fig5.2 key splitting analysis

COMBINING THE KEYS TO REGENERATE THE KEYS:

Before decrypting ,the splitted keys have to combine first to regenerate the original key.With that original key the decryption process is done and the data should be secured.

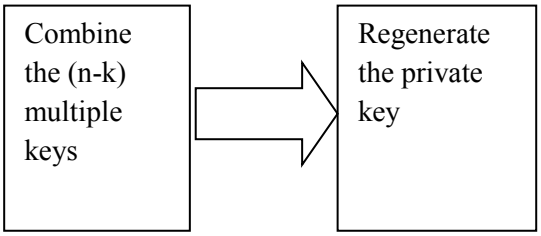
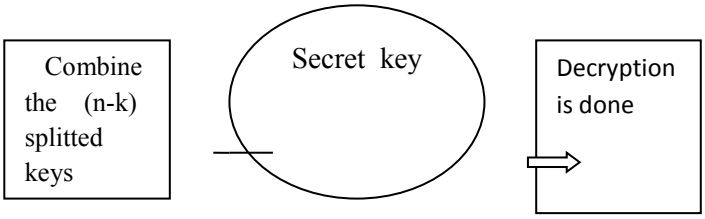


Fig5.3 Combining the keys to rebuild the key

5.4 DECRYPTION PROCESS BY AES:

The decryption is done by using AES Algorithm after combining the keys to rebuild the original key.After decryption the plaintext is recoverd in secured manner.



DECRPTION PROCESS BY AES

VI. CONCLUSION

In this paper outsourcing data to a third-party administrative control entails serious security concerns. Data leakage may occur due to attacks by other users and machines. Data Security for this Environment with Semi-Trusted Third Party, a data security system that provides (a) key management (b) access control, and (c) file assured deletion. Moreover, data leakage and data privacy strategies must be employed so that only authorized users can access and utilize data. Refraining the service providers from utilizing the customer data requires high preventive measures. Encryption techniques provide a solution to ensure privacy and confidentiality of stored data.

VII. FUTURE ENHANCEMENT

The Future of Encryption is very much brighter than past and critical market driver for cryptography which will help encryption and the application. The effective implementation of AES algorithm to encrypt data while sending it to server and Shamir's threshold scheme is used for splitting the keys in safe manner. so implementing cryptography make huge difference in performing and help to implement application which will be secured to avoid threats.

REFERENCES

[1] IEEE security of cloud, Michael Armbrust, Armando Fox,Rean Griffith, Anthony.D "A View of Cloud Computing".

[2] M.Kaufman,"Datasecurity in the world of cloud computing," IEEESecurityand Privacy, Vol.7, No.4, 2009, pp. 61-64.

[3] S.Kamaraand K. Lauter, "Cryptographic cloud storage" Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2010, pp.136-149.

[4] C. Caching and M. Schunter," A cloud you can trust," IEEE Spectrum, Vol. 48, No. 12, 2011,

pp.28-51. 6] W.Diffie, P.C.V.Oorschot, and M.J.Wiener, "Authentication and authenticated key exchanges," Designs, Codes and Cryptography, Vol. 2, No.2, 1992, pp.107-125.

[5] M. S. Blumenthal, "Is Security Lost in the Clouds?"Communications and Strategies, No. 81, 2011, pp.69-86.

[6] Y.H. Hwang and P.J. Lee, "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-User System," Proc.Int'l Conf. Pairing-Based Cryptography (Pairing '07), pp. 31-45, 2007.

[7] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM '11, 2011.

[9] D. Boneh and B. Waters, "Conjunctive, Subset, and Range Queries on Encrypted Data," Proc. Fourth Conf. Theory of Cryptography (TCC'07), pp. 535-554, 2007.

[10] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[11] C. Wang, K. Ren, S. Yu, K. Mahendra, and R. Urs, "Achieving Usable and Privacy-Assured Similarity Search over Outsourced Cloud Data," Proc. IEEE INFOCOM, 2012

[12] E. Shi, J. Bethencourt, H. Chan, D. Song, and A. Perrig, "Multi-Dimensional Range Query over Encrypted Data,"Proc. IEEE Symp. Security and Privacy, 2007.