OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Secure File Sharing In Cloud Using Encryption with Digital Signature

Miss. N. Kanchana[1], Mr. S. Balamurugan[2]
[1, 2] *(PG Student, Assistant Professor, Sri Manakula Vinayagar Engineering College, Pondicherry-605106)*

Abstract: *This paper we discuss about the data sharing in a cloud with multiple owner by generating keys and digital signature. The proposed methodology suggests the encryption of the files to be uploaded on the cloud. To ensure the security of data, we proposed a method by implementing AES algorithm. The integrity and confidentiality of the data is achieved by not only encrypting it but also providing Digital Signature for successful authentication. It provides two way security for data sharing.*
Keywords: *Cloud, Encryption, Integrity, Confidentiality, Digital Signature.*

I. Introduction

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. It comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. "the cloud" is essentially a metaphor for the Internet. Marketers have further popularized the phrase "in the cloud" to refer to software, platforms and infrastructure that are sold "as a service", i.e. remotely through the Internet. Typically, the seller has actual energy-consuming servers which host products and services from a remote location, so end-users don't have to; they can simply log on to the network without installing anything. Cloud computing providers offer their services according to several fundamental models: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

(A) Software as a Service

Delivery of software applications over the internet. The software is frequently delivered using a one-to-may approach and is not customized. Hence on the supply-side, the provider is managing one application from one or more dedicated locations, whilst on the demand-side; customers are not required to make any hardware (such as servers) or software investments. For example: Gmail, hotmail, yahoo.

(B) Platform as a service

Delivery of a computing platform for the development of services and applications from a cloud. This category of service tends to be not as mainstream as the other "-aaS" options. Since it is used almost exclusively by programmers. For example: Google App Engine, Amazon EC2,Microsoft Azure Platform.

(C) Infrastructure as a Service

Delivery and remote management of computer and networking hardware, as well as processing power, as a service over the internet. Customers can purchase storage, processing power, networking capability etc, as and when needed, and commensurate with their actual needs. For Example: Storage-Dropbox, icloud, Adrive, mozy, amazon web service. Web hosting- Go daddy, bluehost, fatcow. Virtual Servers-IBM, Rimu Hosting.

II. Advanced Encryption Standard (AES)

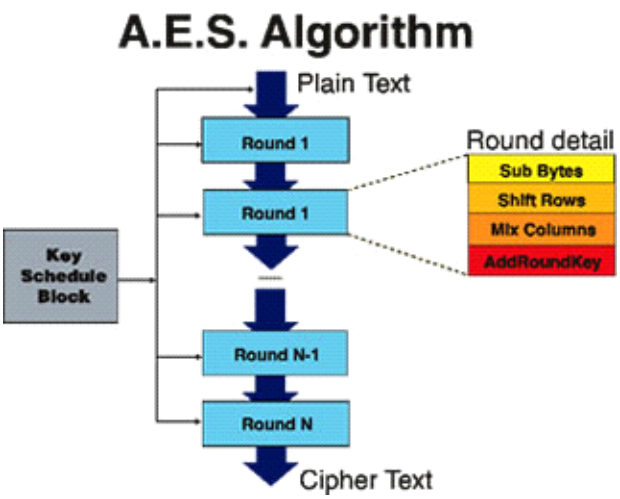
AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

Block length: 128 bits (P = C = {0,1}1 2 8)

Key lengths: 128, 192, 256 bits (K = {0,1}1 2 8 , ...)

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.



(i) KeyExpansion: round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

(ii) InitialRound:

AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

(iii) Rounds:

1.SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

2.ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

3.MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4.AddRoundKey

(iv) Final Round (no Mix Columns):

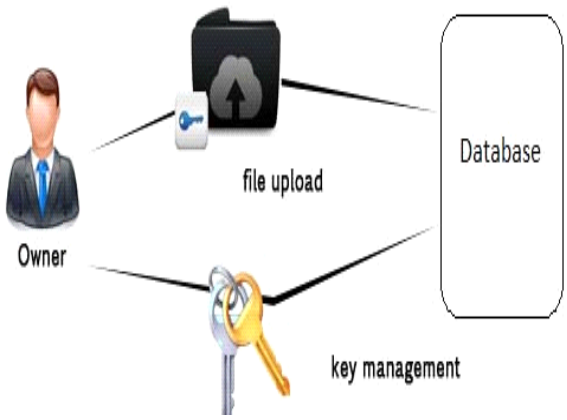
1.SubBytes

2.ShiftRows

3.AddRoundKey.

III. Key Generation

If owner needs to send a file to the user then the unique key will be generated for each user by the owner. Suppose owner would like to send the same file to the different users then the owner can just share the unique key to different users and the owner need not to send the same file again and again. So it eliminates the redundancy in database. If user deletes the file then it won't affect the other users to access that file its because only the key will be deleted not the file. In case if we don't use the key management then it definitely affects the other users to access the files.

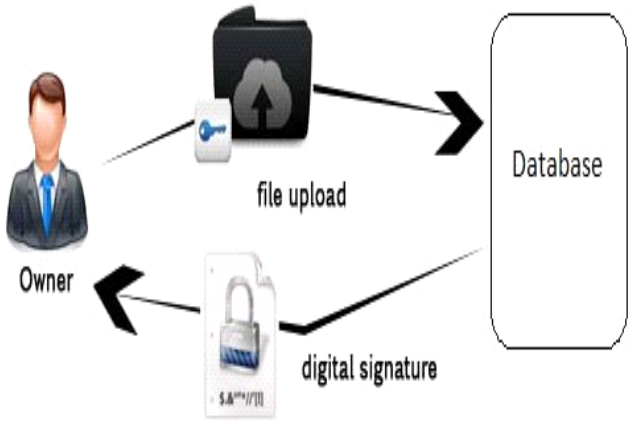


IV. Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering. It is basically a way to ensure that an electronic

document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. Once file is uploaded based on the owner name, user name, key, file name, file type then the digital signature will be created and it is send to the user.



V. File Upload

Steps involved in file upload process are explained below:

Step 1: Accept owner id and password from the owner.

- If owner is authorized,
  then allow to connect with the cloud
- Else,
  show authentication error and don't allow

Step 2: Ask owner to select a file to be uploaded onto the cloud
Step 3: Ask the owner to select a user
Step 4: Ask the owner to enter a unique key for user
Step 5: Apply the encryption algorithm
Step 6: Upload the file on to the cloud
Step 7: The user gets the key through SMS and the Digital Signature file will be generated automatically by the system and it is send to the user through Email once the file is uploaded.
Step 8: Disconnect from the cloud.

VI. File Download

Steps involved in file download process are explained below:

Step 1: Accept user id and password from the user

- If user is authorized,
  then allow to connect with the cloud
- Else,
  show authentication error and don't allow

Step 2: Ask user to select a file to be download which is sent by the owner
Step 3: Ask the user to enter a key which is received through SMS
Step 4: Ask the user to download the Digital Signature file from Email
Step 5: Ask the user to upload the Digital Signature file
Step 6: Check the validity

- If the key and the digital signature is matched,
  then Apply the decryption algorithm for download the file from the cloud
- Else,
  show an error message and reject the download process

Step 7: Disconnect from the cloud

VII. Conclusion

In this paper we mainly focused on data confidentiality and integrity so we used an encryption algorithm and we also designed a digital signature scheme to invoke high secured data transaction in the cloud. It also eliminates the redundancy it's because of key management. Here, anyone could be a owner if they are registered in the cloud. The user of a particular organization can be able to access the particular information which is available in the file. It is more reliable to the cloud for better security.

REFERENCES

[1] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM,pp. 534-542,2010

[3] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian and Aoying Zhou, "Security and Privacy in Cloud Computing: A Survey", In Sixth International Conference on Semantics, Knowledge and Grids, 2010.

[4] Farhan Bashir Shaikh and Sajjad Haider, "Security Threats in Cloud Computing", In 6th International Conference on Internet Technology and Secured Transactions, 2011.

[5] Balachandra Reddy Kandukuri, Ramakrishna Paturi V and Dr. Atanu Rakshit, "Cloud Security Issues", In IEEE International Conference on Services Computing, 2009.

[6] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-55, 2004.

[7] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[8] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu "Plutus: Scalable Secure File Sharing on Untrusted Storage," Pro USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[9] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.