Cloud Security: Using Advance Encryption Standard Algorithm to Secure Cloud data at Client Side and Taking Measures to protect its Secrecy

A Kwofie, AA Barik

Department of Computer Science, University for Development Studies, Ghana

Article Info

Article history:

Received 22 April 2020

Received in revised form 29 May 2020

Accepted 30 July 2020

Available online 15 September 2020

Keywords: Cryptography, Advance Encryption Standard, Algorithm, Message Digest, Cloud.

Abstract: Cloud computing brings a lot of advantages especially in ubiquitous services where everyone can access computer services through the internet. In spite of this, there are key security loop holes that is making users anxious about the safety of migrating to the cloud. This project uses the Advance Standard Encryption Standard Algorithm to encrypt user data at client side before transferring the data to the cloud thereby making encryption key available to only owners of the data. The project also uses Message Digest Algorithm to check for data integrity at client side to know if client's data has been tempered. The project also employs key management technique and backup design to keep encryption keys safety at client side.

1. Introduction

Cloud computing is the practice of using network of remote servers hosted on the internet to store manage and process data rather than a local server or a personal computer. Data on cloud is not completely secure from infection since it is being accessed through the internet. The benefits of cloud computing are many. Some benefits are the portability of the application where users can work from home, work, or at client locations. Moving data into the cloud offers great convenience to user since they don't have to care about the complexities of direct hardware management. Most cloud providers use different models to secure cloud data even in transit and at rest [1]. However, the cloud providers hold the secrete keys on their servers after encryption. This introduces us to a concept known as the "legitimacy of ownership". Who owns the data? Who is to keep the encryption key? This project proposes a model where data will be encrypted using Advance Encryption Standard Algorithm before sending files to the cloud. In addition, Message Digest Algorithm will be used to check the correctness of the data.

2. Related Works

Navia and Chara proposed cloud security model which is based on a three-layer system structure, in which each layer performs its own duty to ensure the data security of cloud layers [2]. The initial layer is responsible for cloud user authentication. It uses One Time Password authentication module and uses digital certificates issued by the appropriate users and also manage user permissions. The second layer manages the user's data encryption by using Advance Encryption Standard Algorithm, which is the most secured and faster encryption algorithm for sensitive data such as one's personal information. Choudhury and Abudin proposes a new authentication system for cloud [3]. As in this technique onetime password is encrypted using public key of user to obtain encrypted onetime password. It removes dependency on third party but limit is its key size.

3. Cloud Computing

Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources. that is, everything from applications to data centers over the internet. cloud computing has made marvelous changes in the functioning and working in information technology sector. cloud computing has also changed the way in which business and personal data are being stored and retrieved using computer, however this has led to many kind of security issues [4]. Via cloud computing, the basic requirements of a customer are provided as a service. software, infrastructure, platform is provided as a service by the service providers. many research scholars and scientist have defined cloud computing at various occasions. [5] has defined cloud computing as follows cloud is a parallel dispersed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and obtainable as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers.

4. Advance Encryption Standard Algorithm

Advance Encryption Standard is a symmetric key block with a data block length of 128 bits, which supports different key lengths of 128, 192 or 256 bits. The number of rounds for key length 128 bits is 10, for key length 192 bits is 12 and for 256 bits 14 rounds. In the encryption of the AES algorithm, each round performs four transformations namely SubBytes, ShiftRows, MixColumns and AddRoundKey, while the final round does not perform the MixColumns transformation. The key used in each round is called the round key. This is generated from the initial key by a separate key scheduling module of Advance Encryption Standard [4].

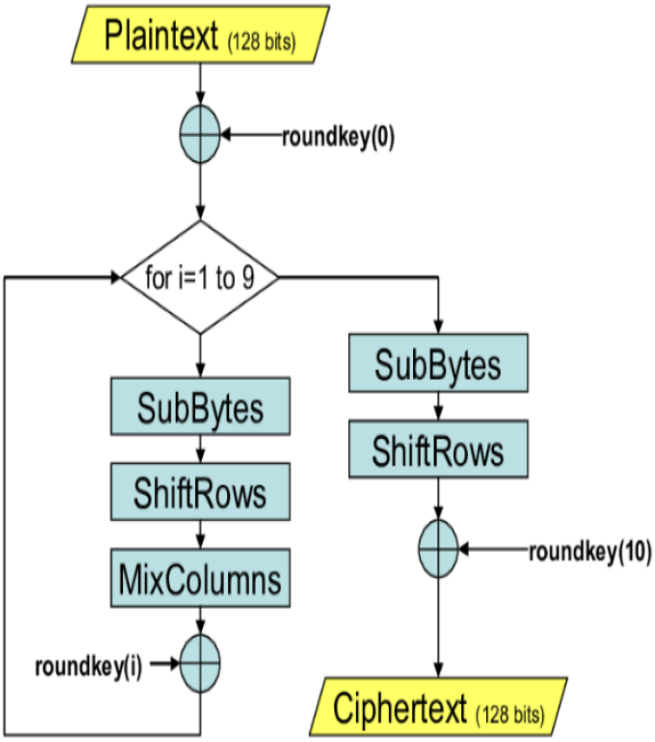


Fig. 1: Advance Encryption Standard Algorithm

5. Message Digest Algorithm

Message Digest (MD5) is a widely used cryptographic hash function with a 128 bits (16 bytes) hash value. MD5 is used in a wide security systems and is commonly used to check the integrity of files. MD5 hash code is expressed as a 32 hexadecimal number. MD5 was designed by Professor Ronald Rivest of MIT to replace an earlier hash function MD4.

Corresponding Author,
E-mail address: arnoldschwazzy@gmail.com

5.1 Implementation

Message Digest processes a variable length message into a fixed length output of 28bits. The input message is broken up into chunks of 512 bit (sixteen 32 bits).

5.2 Step 1: Append padding bits

The message is padded so that its length is divisible by 512. The padding works as follows. First a single bit, 1, is appended to the end of the end of the message. This is followed by as many Zeros as are required to bring the length of the message up to 64 bits than a multiple of 512.

5.3 Step 2: Append Length

The remaining bits are filled up with 64-bit integer representing a length of the original message, in bits.

5.4 Step 3: Initiate MD5 Buffers

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bits words, denoted A, B, C and D. These are initialized to certain fixed constant.

5.5 Step 4: Process the 512 Message Block

The main algorithm then operates on each 512 bits' message block in turn. The processing of a message block consists of four similar rounds. Each round consists of 16 similar operations.

5.6 Step 5: Output MD5 hash code

MD5("I love programming") = 3be898dae0491c568f37962a0d9716c8

MD5("I lov programming") = b9e128ece7c1109a1488ebf86075a58a

Even a small change in the message will result in a mostly different hash code.

6. Proposed Model

The proposed model is the outcome of implementing the advance encryption standard, the message digest and the cloud system as one entity to secure cloud data.

6.1 Client Side Application

The Client Side Application is a software developed in Visual Basic which uses the Advance Encryption Standard Algorithm for encryption and decryption at Client Side. The application also implements the message Digest Algorithm to check for data Integrity as described in the previous chapter. In addition, it has the functionality of managing encryption keys at client side.

6.1.1 Application Window

The application requires the client to input login credentials in order to get access to the system. This step is implemented to keep encryption keys at client side safe.

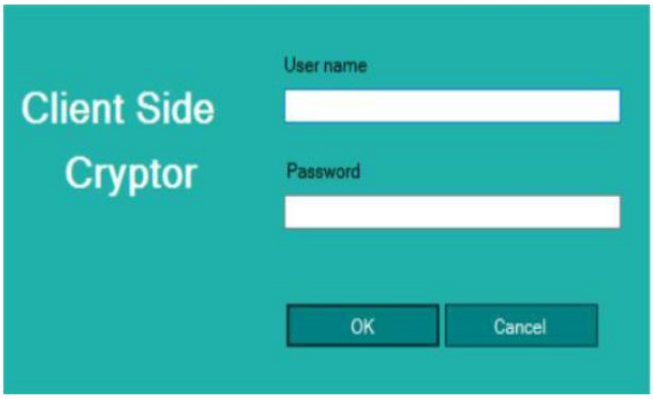


Fig. 2: User Authentication Window

6.1.2 Encryption Window

This window provides a graphical user interface for the users to encrypt their files. It requires the source file, file destination, and encryption key as input. User can generate keys using the generate button or provide his or her own key. The System then encrypt user data using both Advance Encryption Standard and Message Digest Algorithms. The resulting Message Digest 32 hexadecimal code is displayed in the Message Digest text field and concurrently saved in the application's database for key management.

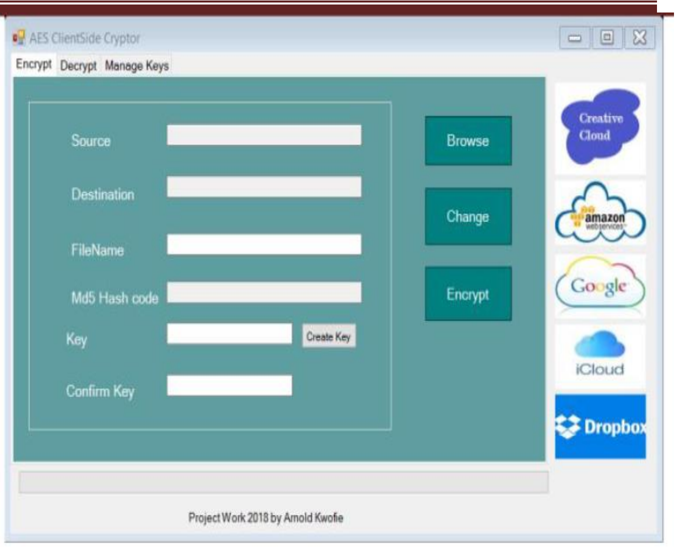
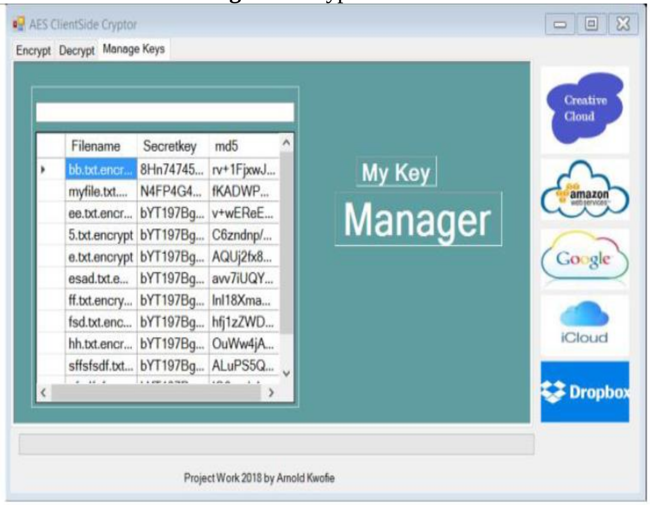


Fig. 3: Encryption Window

Fig. 4: Decryption Window

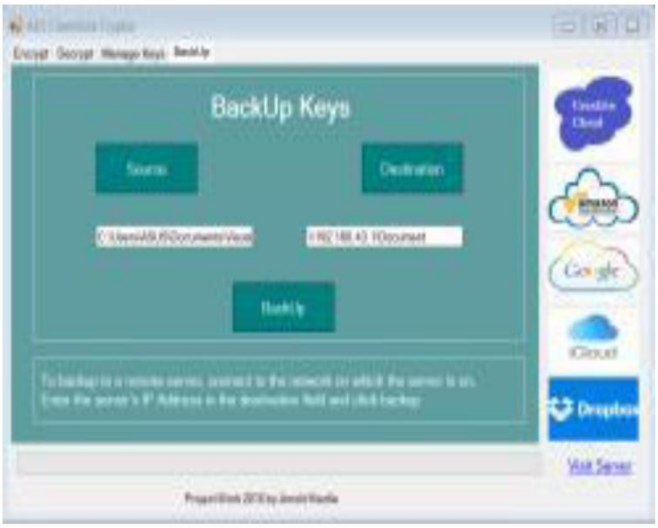


Filename	Secretkey	md5
bb.txt.encr...	8Hn74745...	rv+1FjxwJ...
myfile.txt....	N4FP4G4...	fKADWP...
ee.txt.encr...	bYT197Bg...	v+wEReE...
5.txt.encrypt	bYT197Bg...	C6zndnp/...
e.txt.encrypt	bYT197Bg...	AQUj2fx8...
esad.txt.e...	bYT197Bg...	avv7iUQY...
ff.txt.encry...	bYT197Bg...	Inl18Xma...
fsd.txt.enc...	bYT197Bg...	hfj1zZWD...
hh.txt.encr...	bYT197Bg...	OuWw4jA...
sffsfsdf.txt...	bYT197Bg...	ALuPS5Q...

Key Management

6.2 Decryption Window

Similar to the Encryption widow, the Decryption Window also, requires the encrypted file and it secrete key to decrypt it. After the file is decrypted with Advance Encryption Standard Algorithm, Message Digest Algorithm is again used to encrypt the decrypted file. The resulting 32 hexadecimal code is then compared to the initial hexadecimal code generated during encryption. If both hash codes look the same, the user is prompted with a notification that the file is safe. However, if both hash codes do not look the same, then the file has been tempered. This step checks for data integrity.



To backup to a remote server, connect to the network on which the server is on. Enter the server's IP Address in the destination field and click backup.

Fig. 6: Backup Window

6.3 Key Management Window

Key management window allows the user to access the secret keys used for encryption. The keys are enlisted with their corresponding files and Message Digest hash codes from the application's database.

6.4 Backup Window

The backup window allows clients to backup encryption keys to other storage devices or remote servers through networks. This is important because one cannot tell the uncertainty that could in a way happen to client's machine.

7. Conclusions

In conclusion, the model is described to use Advance Encryption Standard Algorithm to encrypt client data at client side before transferring the data to the cloud. The method also used Message Digest Algorithm to check for the data's integrity. Client will be confident about the state of their data to the cloud because they have the only route to their files.

Acknowledgment

I would like to express my sincere gratitude to Almighty God, for giving me the best of knowledge to accomplish my project aim. I am also grateful to Dr. Alhassan Abdul-Barik who provided me with an opportunity to work under his kind supervision.

References

[1]. Data Protection: Data in Transit vs Data at Rest.(http://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest/), 2017.

[2]. J Navia, K Chara. Data Security Model Enhancement in Cloud Environment, International Journal of Computer Science and Engineering, 2013.

[3]. G Choudhury, J Abudin. Modified secure two-way authentication system in cloud computing using encrypted one-time password, International Journal of Computer Science and Information Technologies, 2014.

[4]. D Purushothaman, S Abburu. An Approach for Data Storage Security in Cloud Computing, International Journal of Computer Science,2012.

[5]. R Buyya, CS Yeo, S Venugopal, J Broberg, I Brandic. Cloud computing and emerging IT platforms: vision, type, and reality for delivering computing as the 5th utility, International Journal of Computer Science and Information Technologies, 2009.

[6]. R Vairagade, S Ugale, P Pedke. Review on 128 bits Advance Encryption Standard Algorithm with Fault Detection, IJAICT. Nagpur, India,2014.