International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Algorithmic Approach to Encrypted Modes of Transmission of Real Time Media in a VOIP Architecture

Toshima Singh Rajput*[1], Kamini Maheshwar[2], Dr. Taruna Jain[3]

*[1]Department of Cyber Law and Information Security, Barkatullah University, Bhopal, Madhya Pradesh, India
[2]Asst. Professor, Department of Computer Science and Engineering, UIT , Barkatullah University, Bhopal, Madhya Pradesh, India
[3]HOD, Department of Cyber Law and Information Security, Barkatullah University, Bhopal, Madhya Pradesh, India

ABSTRACT

Transmission of voice , video and messages over a secured channel of communication has become the priority of the companies emphasising on individualised privacy and support for the customers. Due to an increasing amount of security issues in the VoIP Platform,more technological advances and methods are being exercised to control the security parameters. This research paper is a study of the different modes of encryption of Advanced Encryption standard and generation of Time based one time password. This paper integrates these methods in providing an algorithmic approach to the transmission of voice, video and messages in an encrypted mode in a Client server architectural environment. This research paper integrates the Pycrypto implementation of the AES mechanism. This method is then implemented in a Voice client server architectural environment to provide a secured implementation of three factor authentication mechanism. The process uses the services of a Voice cloud service provider and is a python implementation of the algorithmic approach.

Keywords: AES, TOTP, AES Modes, Plivo API, Pycrypto, Video, Messages

I. INTRODUCTION

Cryptography is a method of protecting data from unauthorized modification or alteration. It is a science of study in which the data to be protected is encrypted using some standardized algorithm. The encrypted data is then decrypted using a reverse process.

In cryptography there are two Algorithms of Encryption and Decryption: Symmetric and Asymmetric algorithm. In Symmetric algorithm the same key is used for encryption and decryption while in Asymmetric different keys are used for encryption and decryption.

In symmetric algorithm two methods are used for creating a cipher text -block cipher and stream cipher. In block cipher data is divided into blocks of text while in stream cipher encryption and decryption is done bit by bit as data is partitioned into bits.

II. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption standard (AES) is a symmetric block cipher program which was developed by National Institute of Standards and Technology (NIST) and was effectively introduced for use by 2002. AES is more secure than the algorithms like DES and Triple DES. It can consume less computing

power and produce high speed encryption. Messages are encrypted using 128,192 or 256 bit keys and it is also called as AES-128, AES-192 or AES-256.The block size of data is 128 bits. There are five modes of operation in AES - ECB, CBC, CFB, OFB and CTR. [1]

A. ECB Mode (Electronic Code Book)

The simplest form is ECB mode of operation. In ECB mode of operation the plain text is divided into **n** number of blocks which is then encrypted with the same key to produce **n** Cipher text blocks. The decryption also follows the same process. Let us assume that the plain text P is divided into P1..Pn blocks and the same key is applied for converting them into cipher text blocks C1...Cn. The reverse

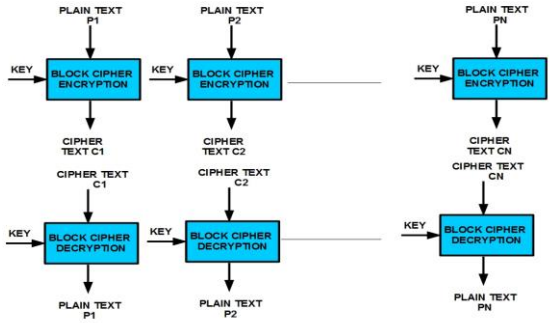

Figure 1. ECB mode of Operation

procedure is the decryption process to convert cipher text into plain text. [2]

B. CBC mode (Cipher Block Chaining)

In Cipher block chaining mode, an Initialization Vector(IV) of the same size of the block is XORed with the Plain text which is then encrypted with the key to produce the cipher text. The resultant cipher text which is again used for the XOR operation with the plain text of the second block and like a chain mechanism the cipher text block is being used to produce the resultant cipher text for the other plain text block. A slight single bit error can result in the corrupted decryption. The initialization vector can be different for any two messages and need not be kept secret which is an advantage for the Code.[2]

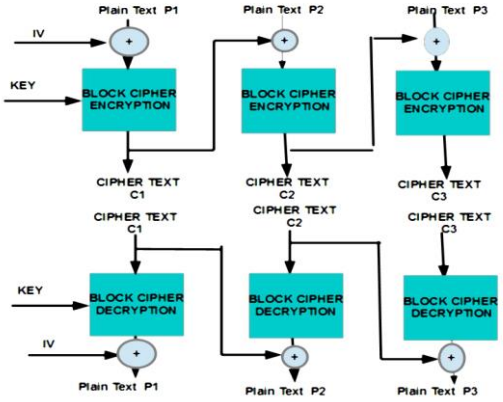

Figure 2. CBC mode of Operation

C. CFB mode (Cipher Feedback)

In this mode of AES encryption, the Initialization vector(IV) is encrypted with the Key to produce the encrypted vector which is then XORed with the Plain text to produce the resultant cipher text. Like CBC mode the cipher text is reused as an initialization vector(IV) to produce the next cipher text block. In the beginning operation the IV(64 bits) is placed in a shift register but the XOR operation is performed with only few bits. The resultant cipher text is placed in the shift register. The CFB mode is considered better as it prevents from Chosen Plain text attacks wherein the attacker attacks the algorithm using a chosen set of plain text attacks. But IV should be unique for every message so that the identical messages does not produce the same cipher text.[3]

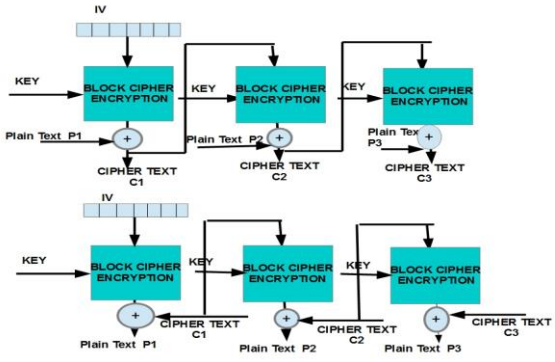

Figure 3. CFB mode of Operation

D. OFB mode(Output Feedback)

In this mode of AES encryption, block encryptor becomes a stream encryptor. In this mode the input

for the shift register for the next block is chosen from the output of the encryptor of the previous block. That is why it is called as Output feedback mode. Error during transmission is limited because only a part of the plain text will be influenced from the error. So this mode is used for communication through media.[3]

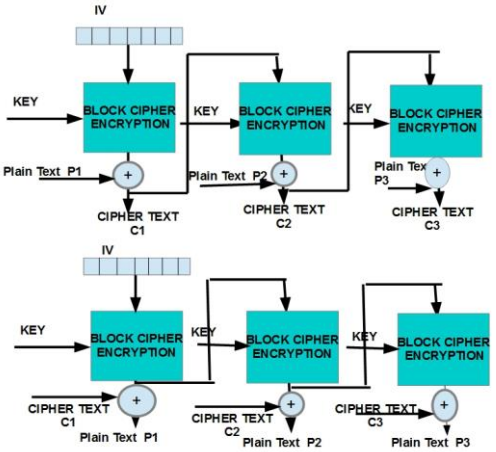

Figure 4. OFB mode of Operation

E. CTR mode(Counter)

In this mode the value of the initialization vector(IV) is a counter with the same block size as the input. Values of the outputs of the next blocks are independent of the result of the previous block thus making it free from propagation error. The value of the counter in the first block is initialised with some value which is incremented by +1 for further blocks. This mode of operation is highly parallelizable and thus can produce faster results.[3]

The ECB mode of AES is considered as primitive because of its simple implementation and is considered as insecure.The CBC mode is much better as compared to ECB and is used in many of the Secure Socket Layer /Transport layer Security (SSL/TLS)cipher algorithms. CBC mode is under attacks and cannot be implemented without a proper set of integrity checks**.** The advantage of using CFB is you only need the encryption transform and not the decryption transform. It is parallelizable too.

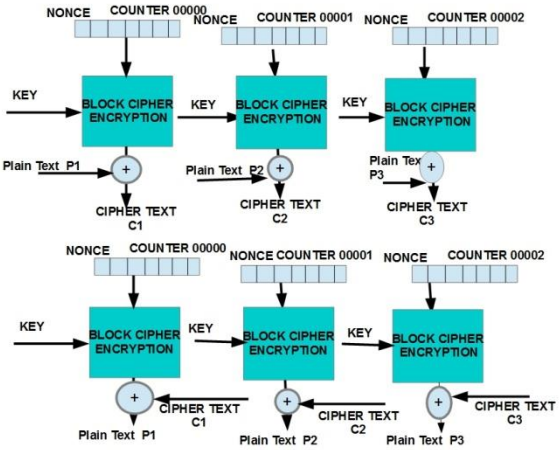

Figure 5. CTR mode of Operation

III. TIME BASED ONE TIME PASSWORD (OTP) ALGORITHM

Time based one time password (TOTP)algorithm is based on the IETF RFC 5238 industry standard HMAC-SHA1(Hash based Message authentication code Secure Hash algorithm) token algorithm. The current timestamp and the SHA algorithm is combined to generate a one time password. In this algorithm the system TOTP validation server uses the system time to generate OTP. To consider the time drift the Network Time protocol on the Cloud servers must be considered. Time differences between the TOTP validation server and the mobile devices can result in the mismatch and the algorithm may cease to work. So the mobile devices has to be configured according to the network service providers. To allow the time differences a time-step of 30 seconds is allotted as a valid time setting for the received OTP to match with the server generated OTP. Sometimes the network latency, time drift has to be considered so the time step of 30 seconds is introduced as a timestamp which increments in a 30 second interval. The OTP will be used as a Two Factor authentication process.[4] [5]

IV. PROPOSED WORK

The proposed algorithm is used to make voice calls and send messages using the voice cloud service Plivo. The client server architecture creates an environment in which the user logs in an authenticated environment using username and password. The cloud service provides an authentication to each and every user with a Authorized ID and Token which is used to login from any interface to the Plivo Cloud service. The figure below depicts the entire architecture of how an encrypted OTP using AES algorithm can be used to create a secure client server architecture environment.

The user agent A in a VoIP Cloud makes a call to Client B by sending an encrypted OTP using AES CFB mode of operation. The webserver then decrypts the OTP and sends it to the client B. The Client B types the OTP in the API and then sends it to the webserver. The Webserver matches the OTP and the call is established between the two clients. This SMS generated OTP can be regenerated at every 30 seconds interval from the client API and compared with the webserver Clock. Pycrypto is a python library which provides algorithms like AES,DES,SHA for encryption and decryption. Thus the algorithm for the above architecture is as follows.

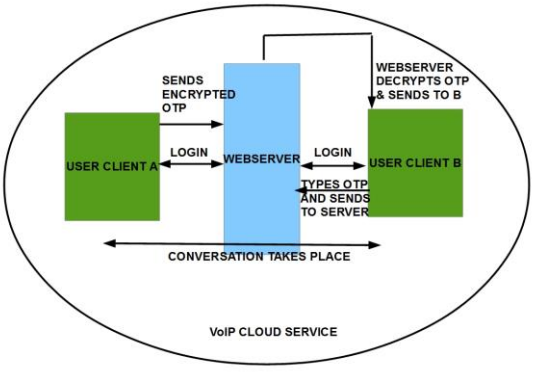

Figure 6. A Secured Client server architecture using OTP and AES

1. Algorithm

Client API

Step 1: Accept the number to dial the call
Step 2: Initialize the Authorized ID and Authorized Token with the value specified during login in a Plivo API.
Step 2: Login through the Authorized ID and Token.
Step 3: Call function "send OTP"
Step 4: If OTP does not match goto step 3
Else
Step 5: Initialize the parameters of the call function (time limit, answer URL)
Step 6: Make the call
Step 7: Print the call response on the screen

Send OTP Function

Step 1: Login through the Authorized ID and Token.
Step 2: Choose the mathematical random function to choose number in the range of 10000 to 99999
Step 3: Initialize the object variable with the IV and the key pair using mode AES CFB.
Step 4: Encrypt the chosen number with the object variable with Pycrypto function encrypt .
Step 5: Send the SMS of the encrypted code to the webserver.

Webserver

Step 1: Get the senders phone number
Step 2: Get the receivers phone number
Step 3: Initialize the object variable with the IV and the key pair using mode AES CFB.
Step 4: Decrypt the object variable with Pycrypto function decrypt.
Step 5: Send the code to the Client B as receivers phone number
Step 6: wait for the client response
Step 7: If the OTP received does not match send a signal to the client to regenerate OTP
else Send true to the client A

The code used in python Client API for Sending an OTP is

```
obj = AES.new('This is a key123', AES.MODE_CFB, 'This is an IV456')
ciphertext = obj.encrypt(str(code))
```

The python implementation of the webserver will decrypt the code using the following code

obj = AES.new('This is a key123', AES.MODE_CFB, 'This is an IV456') decryptext=obj.decrypt(text) # to decrypt the text and forward it to other client

Figure 7. Result generated on the Linux environment on making calls

V. RESULT

Client server architecture is able to make calls by sending OTP to the client but in a decrypted form. The output as shown in the figure was discovered when the calls were established between the two clients. The AES mode of encryption provides a secured environment to provide a peer to peer encryption mechanism for the Client in a VoIP cloud service. As many times the call was established the Request UUId parameter, aleguuid parameter to set up a call every time changes as enlisted with the call fired message on the screen.

VI. CONCLUSION

The encrypted modes of transmission provides a three factor authentication and provides an advanced approach to look into the parameters of security which pose a threat to the daily voice calls made in a Corporate network. The customers privacy and support is the ultimate motive behind each and every parameter of call set up and call management. With these criteria a secured architecture can be created with the separation of voice and messages to provide a strong network architecture. Security of the calls made using a VoIP architectural platform is the major concern of Security industry nowadays.

VII. REFERENCES

[1]. Anita Dashti, Hashem Alvandi Kheradmand, Mohammad Davarpanah Jazi, "Comparison Of Three Modes Of Cryptography Operation For Providing Security and Privacy Based on Important Factors", International Journal of Information Technology and Electrical Engineering,ITEE, 5 (3), pp. 7-12, jun 2016

[2]. Dobre blazhevski, Adrijan bozhinovski, Biljana Stojchevska, Veno Pachovski, "Modes of Operation of The AES Algorithm ",The 10th Conference for Informatics and Information Technology (CIIT 2013) pp 212-216

[3]. Mohan H.S and A. Raji Reddy, "Revised AES And its Modes Of Operation", International Journal of Information Technology and Knowledge Management, January-June 2012, Volume 5, No. 1, pp. 31-36

[4]. K Marimuthu, D Ganesh Gopal, Harshita Mehta and Aditya Rajan, P Boominathan, "A Novel Way Of Integrating Voice Recognition and One Time Passwords To Prevent Password Phishing Attacks", International Journal of Distributed and Parallel Systems (IJDPS) Vol.5, No.4, July 2014

[5]. Mohsen Gerami, Satar Ghiasvand,"One-Time Passwords via SMS ", Bulletin de la Société Royale des Sciences de Liège, Vol. : 85, 2016, p. 106-113

[6]. Getting Started with Plivo, https://www.plivo.com/docs/getting-started/

[7]. PyQT4 Reference Guide, https:// pyqt.sourceforge.net