Securing iClouds Storage Based On Combination of RSA and AES Crypto System

Badreldin O. S. Elgabbani *boelgabbani@uqu.edu.sa*
MCC/ Dep. Of Engineering/computer
Umm Al-Qura University
Makkah/ 21955/Saudi Arabia

Emad Abdulrahman Shafie *eashafie@uqu.edu.sa*
MCC/ Dep. Of Engineering/computer
Umm Al-Qura University
Makkah/ 21955/Saudi Arabia

Abstract

The strength and consistency of cryptographic systems in application, development is highly significant to reduce the penetration chances of applications and files storages. Nevertheless, the data protection systems still face challenges to protect those systems from being attacked. This research has been designed to protect highly important documents saved in iClouds computing storage from being exploited through illegal techniques. The research proposes a new method of encryption that combines two of the most familiar techniques, which are based on (RSA) model invented by Rivest, Shamir, and Adelman merged with an Advanced Encryption Standard (AES). The new combination RSA and AES method will be used on iCloud storages to give them more security and effectiveness as compared to standalone encryption. The main idea of the new technique is to choose two big unpredictable prime numbers at random for public and private key merging with trusted and widely used AES procedure. The research will be applied and evaluated by using a case study to show the new suggested method. Moreover, the case study will be run on iClouds technique namely drobox.

Keywords: Encryption, Decryption, iCloud, Combination.

1. INTRODUCTION

A number of ways and protocols are used to transfer files on the Internet for exchange of significant information in different fields, like international trade, commerce and industries, and secret military organizations.

Icloud storage is one of the most important ways of sharing and transferring files on the Internet .[1] Shared access to Icloud storage requires that the shared files are secure and access to the specific files is restricted to and controlled by the files owner. Encryption is a common technique to control the use of shared files or data, and it grants privileges to known users.

Researchers dealing with crypto graphics propose a lot of papers and ideas that concern encryption and decryption of files and data [1,2,3]. RSA (Rivest, Shamir ,and Adleman), and AES (Advanced Encryption Standard) algorithm are the most common and widespread techniques that are used to encrypt files. They will be discussed in detail later in this paper. This paper discusses the effectiveness of combination of those techniques and our suggested case study shows the extent of their success.

The paper comprises the following sections, Section 2 provides Literature review of cryptographic, RSA and AES. Section 3 illustrate our research methodology and describe how our proposed model will be designed. Section 4 will discuss a case study that illustrates

combination experiments of encryption RSA and AES algorithms, and in Section 5 discusses the results and gives a conclusion and suggested future work .

2. LITERATURE PREVIEW

2.1 Cloud Computing

iCloud computing generally defined by the National Institute for Standards and Technology (NIST) (Badger et al., 2011) “cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". This achievement represents a real genitive, to Information security systems.

The iCloud technique is one of the greatest inventions of the new era, which makes high cost devices, top security software, enabled for everyone, and offers the possibility to follow the evolution of hardware and storage containers, the main idea for iCloud security is to encrypt files before uploading.

2.2 RSA Background

The importance of encryption has been noticed since ancient times, so to maintain the privacy of individuals, security of nations Also it is a highly important for industrial facilities, commercial products, military and the transfer of high-confidential information. The main purpose of encryption is to preserve country from the scourge of wars, intellectual information rumors and Infringement of industrial inventions.

Many encryption methods have been tested and applied, but the most famous one is RSA encryption technique it is invented in 1978 by Rivest, Shamir, and Adleman. These encryption techniques are helped to speed encrypted of explicit texts to crypto text and vis versa[1,2,3,7,8].

2.3 The RSA Algorithm: An Overview

Depends on choosing any two primes numbers p and q, s can be defined as s=p*q and choosing L such that L and φ(s) are prime, (L, φ(s)) = 1. where p, q are prime; s and L are public.

Firstly, text should be transfer into decimal number using ASCII. If the text size larger than s, it should be distributed into blocks in smaller parts than s. These blocks are labeled b_1, b_2, · · · ,b_r. In theory, it could happen that some b, s is not relatively prime. [1,2,3,7,8].

2.4 RSA Algorithm

Generate two large random primes, p and q Compute $n = p*q$.
Compute $\phi(n)= (p - 1) *(q - 1)$
Find public key e such that $1 < e < \phi(n)$.
Find private key d such that $1 < d < \phi(n)$. Satisfying extended Euclidean algorithm
$gcd(e, \phi(n))=1$
$e*d \bmod \phi(n)=1$
Encryption and decryption main steps $M^e \bmod(p*q)=C$
$C^d \bmod(p*q)=M$

TABLE 1: RSA Algorithm [2].

2.5 Fundamentals of AES

In 1997, NIST announced a challenge for the successor to DES. To allay the suspicions that the NSA had placed "back doors" in DES [9], the competition was to be open and public, and the encryption algorithm was available for use royalty-free worldwide.

Due to that challenge AES was classified for use with high information via the world, it is defined as a symmetric block cipher, operating on fixed-size of data. AES supports 128-, 192-, and 256-bit keys. The length of these keys gives an advantage for resisting attempts to decrypt encryptions keys [4].

2.6 High-level Description of The Algorithm

For round =1..... step 1 to Nr-1 do SubBytes(state)
ShiftRows(state) MixColumn(state)
AddRoundkey(state,w[round*Nb,(round+1)*Nb-1] End for
SubBytes(state)
ShiftRows(state) AddRoundkey(state,w[round*Nb,(round+1)*Nb-1])
Out=state End

TABLE 2: AES algorithm [5,6,10].

2.7 Sub Bytes According To Look Up Transfer Table

Sub Bytes transform is a simple transform, which encipher 8 bit data to other 8 bit data determining the multiplicative inverse for a given number in GF(28).

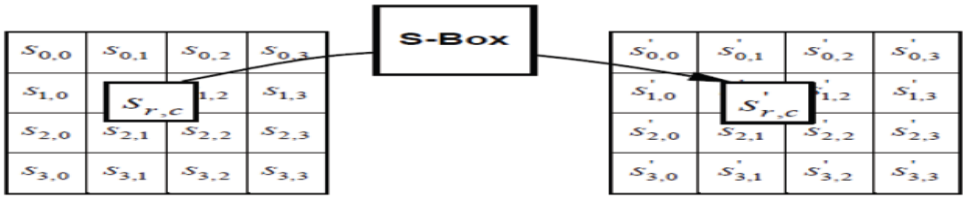

FIGURE 1: AES Sub Bytes' Technique.

2.8 Shift Rows

Shift rows is used to shift rows by certain offset technique shows below.

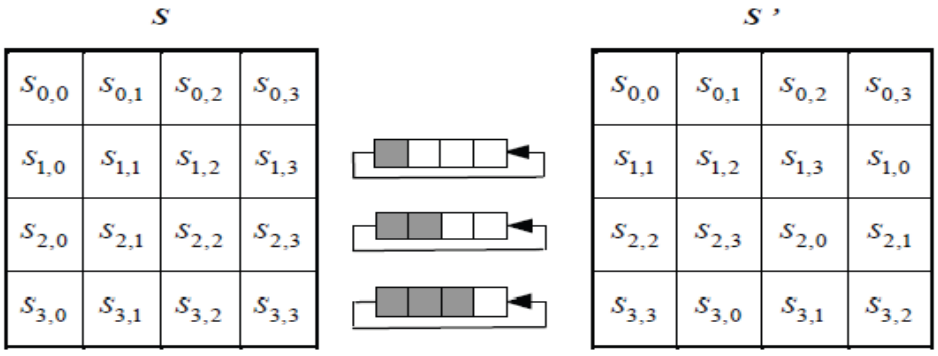

FIGURE 2: Shift Rows Technique.

2.9 Mix Columns

In the Mix Columns, combined each column by using an invertible linear transformation

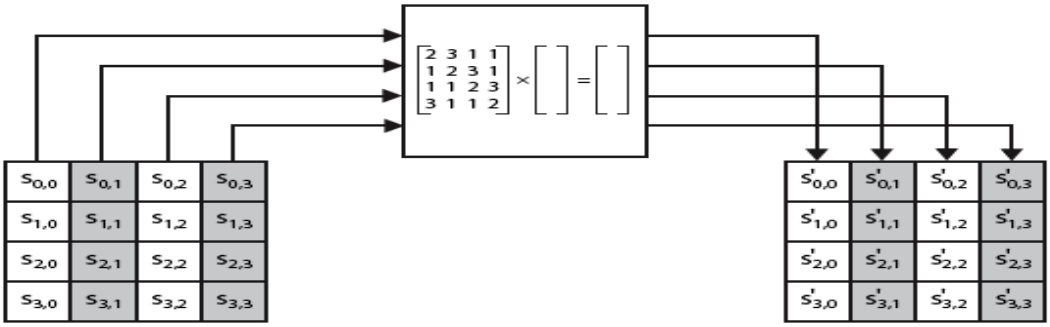

FIGURE 3: Mix Column Technique.

2.10 Add Round Key

The sub key added by using bitwise XOR that combined each byte of the state with the corresponding byte of the sub key

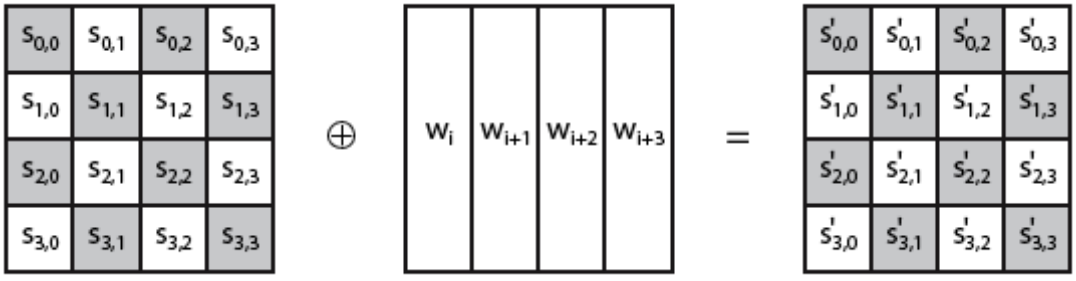

FIGURE 4: Add Round Key Technique.

3. METHODOLOGY

It's observed that the data protection methodologies faced a big challenge to protect the information system, nevertheless the strength and consistency of cryptographic systems gives penetration opportunities almost non-existent.

Here is a combination RSA and AES method that used in iCloud technique; it is more powerful than RSA or AES standalone.

The method based on RSA encryption system, merged with an advanced encryption standard AES.

It's main objectives to provide high secure for important messages by choosing randomly and unpredictable two big prime numbers for public and private key merging with trusted and widely used AES procedure.

3.1 Combination of RSA and AES Crypto System Model

1. Receiver generate public and private key using RSA algorithm
2. Receiver send public key to sender
3. Sender encrypt his message using AES algorithm
4. Sender encrypt the round key using Public key
5. Receiver decrypt the round key using private key
6. Receiver decrypted the whole massage using AES technique

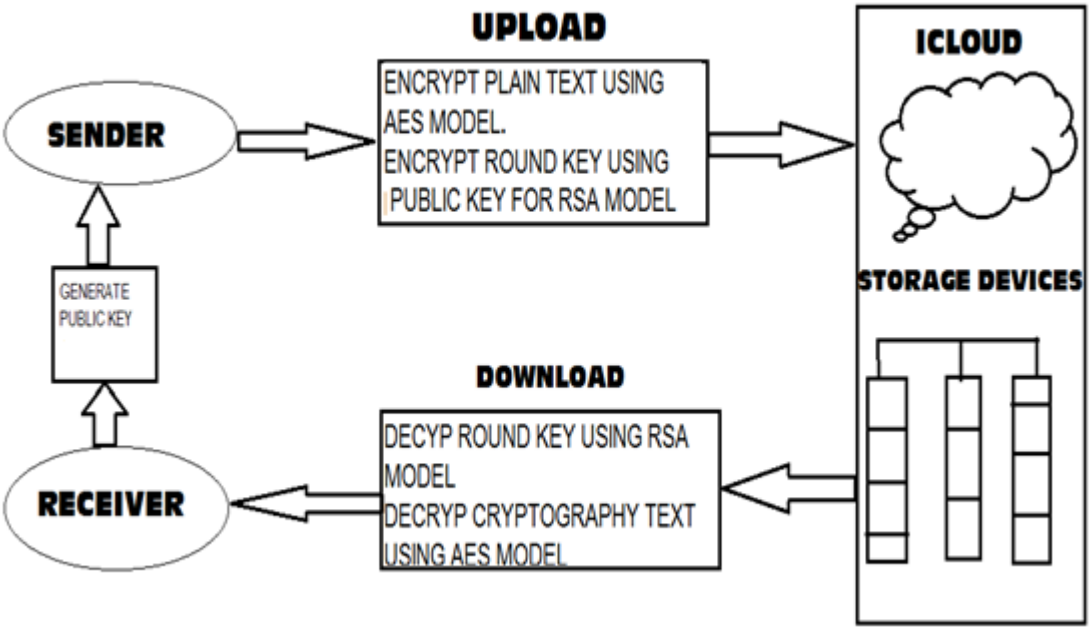

FIGURE 5: AES and RSA Combination Encryption System.

4. PROPOSED MODEL

Overview of network architecture for cloud storage service architecture is illustrated in Two different network entities can be identified as follows:

Receiver: an entity, which is used to retrieve the data from cloud server.

Sender: an entity, which is used to upload data to the cloud Server (CS): the cloud server is an entity, which is managed by cloud service provider (CSP) to provide data storage service and has

significant storage space and computation resources Receiver generate public key and private key using RSA model then make the public key available to senders.

A] Sender encrypt his plain text using AES system.
B] Sender encrypts his AES symmetric key using the public key.
C] Receiver decrypts the AES key using his private key then decrypt the cipher text.

4.1 Case Study

Makkah community college MCC keeps all it's important documents including self-study report concerning academic accreditation, so as to submit it to the (USA council of occupation education) in the drop box through iCloud technique.

MCC folder in the drobox being used as a cases study for this research concerning the combination of RSA and AES for encryption system techniques through the following steps.

1- The receiver generates public key (n, e) and private key (n, d) it sends the public key and receives encrypted message contains round key need to be decrypt so as to decrypt the whole message.

Satisfying e*d mod (p-1) *(q-1)=1

```
Declare keyname;
    Call RSACryptoServiceProvider;
        Generate Public, private keys;
```

2- The Sender use the public key to encrypt the first round key, used in AES encryption procedure by the public key

```
Use RSACryptoServiceProvider to
enrypt the Rijndael key.
    RSA is previously instantiated:
        byte[] keyEncrypted = rsa.Encrypt(rjndl.Key, false);
```

3- The Receiver decrypt the round key then decrypt the whole encrypted passage

The receiver gets the message and then should have to decrypt the key so as to get the original round key after that he can encrypt the whole file the following c# interface reflect that steps.

The AES Algrithm start by adding the round key and the procees will be due to 9 rounds five stages

The AES algorithm applies to both encryption and decryption. The process for encryption starts by adding the round key followed by 9 or 10 rounds of four or three stages respectively. The same process applies for decryption in inverse stages.

The sender use AES technique to encrypt his massage

3.1 Create instance of Rijndael for symmetric decryption of the data.

3.2Generate byte arrays to create the round encrypted key.

3.3Construct the file name for the decrypted file by using File Stream to read the encrypted input file (inFs) and save the decrypted text into output file (outFs).

Convert the lengths to integer values Create the byte arrays for the encrypted Rijndael key, and the cipher text.

Extract the key and IV

3.4 Use RSACryptoServiceProvider to decrypt the Rijndael key.

3.5 Decrypt the key will be followed by decrypting the whole cypher text into the file stream.

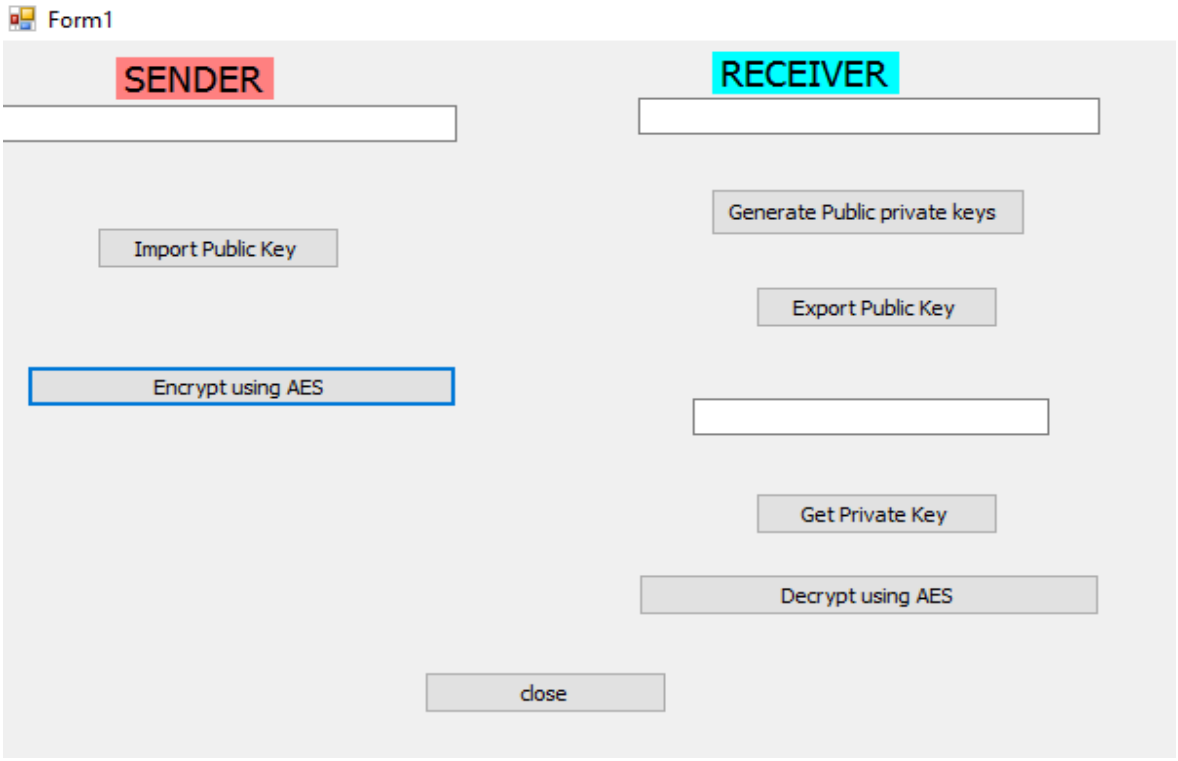

FIGURE 6: AES and RSA Combination Interface Design.

The receiver uses this interface to generate two keys, Public and private keys, he sends the public key to senders and keep private key so as to encrypt sender's message.

The sender encrypts the AES round key by RSA system using his public key. after that he encrypt the whole message using AES system.

The receiver decrypts the round key using the private key after that he decrypts the whole file using AES system here we observed that the key size has been chosen to be 128 bit and the block size is 256 bit so as to use Rijndael special case of AES technique, which is quiet enough for our case study.

```
rjndl.KeySize = 128;
        rjndl.BlockSize = 256;
        rjndl.Mode = CipherMode.CBC;
```

Encrypted File

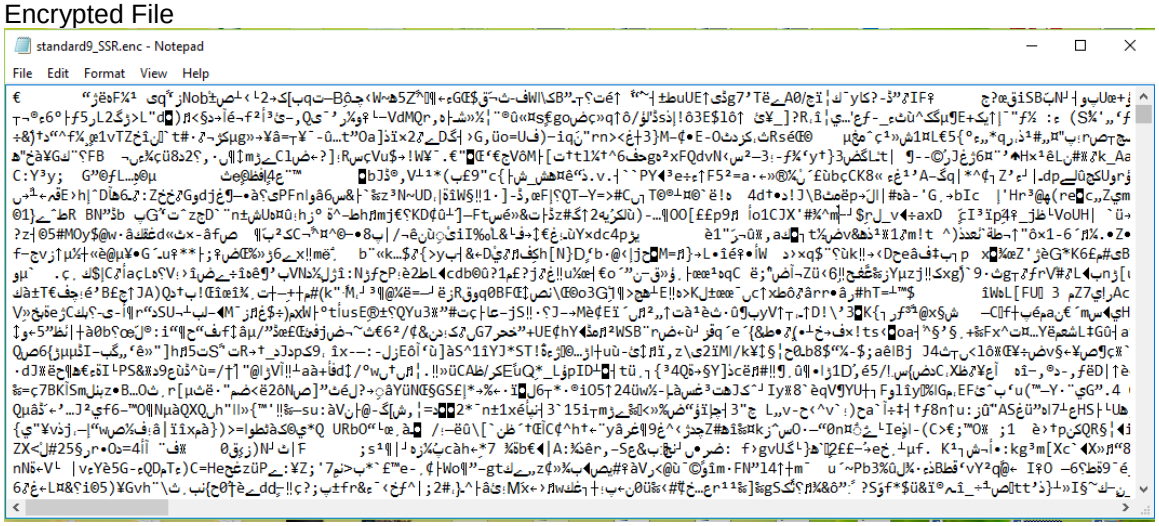

FIGURE 7: Encrypted File.

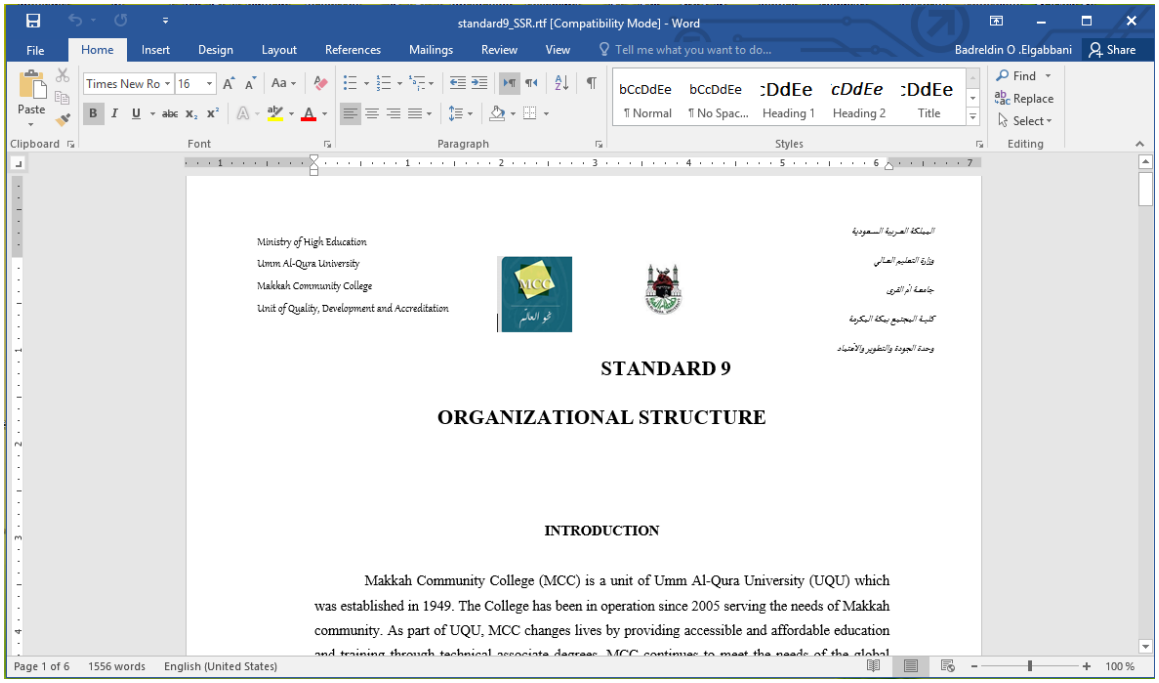

FIGURE 8: Decrypted File.

5. RESULT DISCUSSION

The case study concerns 10 academic standards chairmen, distributed in different places and different devices on the Internet, there by the public key should be available via Internet and the private key held by the academic coordinator the one who can turn the crypto texts to the plaintext.

We used RSA encryption asymmetric keys that are used to different public and private variables of sizes, making it difficult to penetrate the text blinded and is less vulnerable to attacks from the secret key to replicate easy guessing and penetration.

We used non-symmetric encryption algorithm to encrypt a symmetric secret key, and by this procedure the following steps are achieved.

1-Hierarchical system used to protect data
2-Powerful combination system including RSA and AES are being used to protect the information
3-Avoiding RSA disadvantage, by applying RSA encryption system only on the shortage amount of data, representing the round key, on the other hand benefit of the powerful of AES encryption system
4-Avoiding the weakness of AES symmetric key, and on the other hand benefit from the powerful of the rotating of blocks of AES system.

It is observed that the secret AES symmetric encryption method, used one similar key held by the two members and this key may send via web sites protocols, so this key is easily accessible via cryptographic analysis methods, and faced brute attack method, that used to apply each expected key on a piece of crypto text, even up to the explicit text.

The study dealt with the use of the RSA system, to generate the public key and the private key, and then send the public key to encrypt the round key of the system and then used to encrypt the whole of the content, then the receiver decrypts the round key using his private key, and thus decrypts all the content, It is a great and powerful work, but like other models, which focus on the means of symmetric key, often exposed to the middle man attacks, used to stay between devices and servers, and hunts the public key, and change it, followed by decrypting the round key and the rest of the data.

This problem leaved to be deal with by professional web sites security applications.

5.1 Future Study

We suggest indepth mathematical studies using existing protocols like Certificate Authorities CA [11]. And Transport Layer Security/ Secure Sockets Layer (TLS/SSL) in securing the data traffic between clients and servers[12].Transoport Layer Security (TLS) protocol is used primarily to provide privacy and data integrity between two or more computer communicating applications when secured by TLS.

6. REFERENCES

[1] Cutler, Matthew, and David Greenstein. "System and method for social interaction, sharing and collaboration." U.S. Patent Application No. 13/465,572.

[2] Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and PublicKey Cryptosystems". MIT. 1977.

[3] Robinson, Sara. “Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders.” SIAM News, Volume 36. June 2003.

[4] Rijndael "Advanced Encryption Standard (AES)" FIPS. November 23, 2001.

[5] Morris J. Dworkin, Elaine B. Barker, James R. Nechvatal, James Foti, Lawrence E. Bassham, E. Roback, James F. Dray Jr." Announcing the Advanced Encryption Standard (AES) " NIST (2001).

[6] Nicolas Courtois, Josef Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". pp267–287, ASIACRYPT 2002 Web sites references.

[7] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2.

[8] R.L. Rivest, A. Shamir, and L. Adleman . "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"(accessed December, 5, 2019) http://people.csail.mit.edu/rivest/Rsapaper.pdf.

[9] Federal Information Processing Standards Publication 197 November 26, 2001. "Announcing the ADVANCED ENCRYPTION STANDARD (AES) " https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[10] Online Domain Tools is a project of AITIS s.r.o., a privately held Czech Republic company "AES – Symmetric Ciphers Online" http://aes.online-domain-tools.com/ (accessed January, 21, 2019).

[11] Zakir Durumeric; James Kasten; Michael Bailey; J. Alex Halderman (12 September 2013). "Analysis of the HTTPS Certificate Ecosystem" (PDF). The Internet Measurement Conference. SIGCOMM. Archived (PDF) from the original on 22 December 2013. Retrieved 20 December 2013.

[12] T. Dierks; E. Rescorla (August 2008). "The Transport Layer Security (TLS) Protocol, Version 1.2". Archived from the original on 2017-12-24.