Improve Security of Cloud Storage by Using Third Parity Authentication, One Time Password and Modified AES Encryption Algorithm

Firas A. Abdulatif *[1], **Maan Zuhiar**[2]
[1]College of education Ibn Al-Haitham, Informatics Institute for Postgraduate, Iraq
[2]Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate, Iraq

Article Info

Article history:

Received Jan 21, 2018
Revised Mar 4, 2018
Accepted Mar 11, 2018

Keyword:

Cloud attacker
Cloud security
One time password
Security of cloud storage
Third parity

ABSTRACT

Cloud computing is a new term to provide application and hardware as service over the internet. Demand for cloud has increased dramatically in recent years. However, a major drawback for cloud adoption is lack of security so that we will try to solve some security issues related to cloud storage by design and implement a secure system to store privet data in cloud storage. This secure system provide secure login to cloud by using third parity authentication (smart phone) and one time password depend on chaotic system to prevent unauthorized people from get access to cloud and modified AES algorithms to encrypt the data in the cloud storage.

Corresponding Author:

Firas A. Abdulatif ,
College of education Ibn Al-Haitham,
Informatics Institute for Postgraduate, Iraq.
Email: jahangir@southern.edu.bd

1. INTRODUCTION

Cloud computing is a new technology that aimed to make software, hardware and computational resources available as services on demand, in a short time and the cost based on the amount of resource used. There are three service models offers by cloud: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The main goal of cloud computing models is to decreasing operational costs and above all let IT department’s emphasis on strategic projects rather than only keeping their datacenters working [1]. Cloud computing has created a quantum leap in the information technology industry and provides many benefit such as on demand self-service, broad network access, resource pooling, fast elasticity, and measured service. These benefits enabled cloud to have important effect on different sectors of developed cites [2]. The deployment models of cloud computing are: Public cloud, Private cloud, Community cloud and Hybrid cloud. Public cloud is offered for the public use and it’s a cost effective service for applications hosting. Few examples are: Google, Amazon and Microsoft. Mostly Private Cloud is used. It is appropriate for a single organization. Community cloud is used by a set of organizations that have common interests. Hybrid cloud is a merge of private with public Cloud model in order to provide several different functionalities within the same company[3]. In 2016 financial investment on cloud computing will be Global compound annual growth rate of IaaS 41%, PaaS 26.6% and SaaS 17.4% [3].

Cloud computing has big effect on developed cities. Government G-clouds are promising models for developed cities that can reduce IT costs and deliver platforms for small business applications. The UK government’s G-cloud is an exemplary initiation in this regard. Cloud computing gives opportunity to design different services which can support the necessities of developed cities such as cloud-based intelligent car parking service and developed city logistics. In addition, it has the potential to centralize the World's computing power. This will have an effect on reducing consumption of energy, which is one of the main sectors of developed cities. Cloud computing is also opening new possibilities in virtualizing physical spaces and substituting by digital ones [2].

This paper contain in addition to section one section two, will present the cloud computing security attack, section three will present proposed system design, Section four will present result the proposed system and section five will present the conclusion of the of this paper.

2. CLOUD COMPUTING SECURITY ATTACK

Cloud computing offers a variety of services including storage. Cloud storage has many drawbacks one of this Loss of Physical Control such that user cannot access their data, these results in a range of concerns:

a. Control over user data or organization data may be comingled in various ways with data belonging to others [4].
b. Insecure APIs and interfaces:
c. There are group of APIs or software interfaces provided by cloud suppliers for users to control and interact with services provided by the cloud. The availability and security of cloud services is rely on the security of these basic APIs. This APIs must be designed in a security way to protect against attacks and malicious attempts to circumvent policy. Organizations build upon these interfaces to offer additional services to their customers
d. Malicious Insiders
e. The malicious insiders is amplified for customer of cloud by the convergence of IT services and customer under a single management domain
f. Data loss or leakage
g. The process of alteration or deletion data without keeping a backup of the original copy, data will be loss. Illegal users must be block from access to sensitive data [5].
h. Denial of service
i. The denial-of-service attack block legal users from accessing their data. The denial-of-service attack can alter the encryption key or slow the system to block users from using the service by trying to use the wrong password more than once. Therefor cloud service providers should develop a mechanism so that the attackers cannot impact on the services provide by the cloud[6].
j. Vendor lock-in:
k. One of the concerns that is often overlooked when choosing a cloud provider is vendor lock in: cloud service provider block the services provided to the customer such that customer cannot access his data and use any services provided by the cloud or cannot move data to other provider.
l. SQL injection:
m. It is done by inserting SQL orders in a database of an application from the web to Smashing that database.
n. Guest-hopping attack
o. The attacker tries to access to virtual machine by breakthrough other virtual machine hosted in the same hardware. The characteristics of public cloud computing are define by multiple rentals and shared resources. This type of attackers exploits the failure of separation mechanisms that used to separate the usage of storage and hardware [7]
p. Brute force attack
q. A brute force attack used to get user information such as a password, or personal identification number. An automatic software in a brute force attack is used to generate a big number of consecutive guesses as to the value of the desired data. This type perhaps used by security analysts to test an organization's network security or by criminals to crack encrypted data [8].
r. Account or Service Hijacking
s. Is a ways of fraud, phishing and vulnerability exploration moreover password credentials used in distributed methods give breadth to this problem. The anxiety with abduction of accounts was the goal of many cloud service providers already consolidated in the market, such as Amazon.

3. PROPOSED SYSTEM FOR CLOUD STORAGE

The proposed system make security to login process and stored data in the cloud storage increase by using third party authentication and one time password and encrypt store data by modified AES algorithms .

Here used smart phones as a third party because they are personal devices used by the owner only, stay with him wherever you are and one time password to identify people who have permission to access and using cloud facilities which is only usable for one time to prevent unauthorized persons from access, alter and manipulate user's data and expiry after half hour until if not used. These onetime passwords go to the third party to make sure it only reaches to the authorized person. Figure 1 Explain the general structure of the propose system.

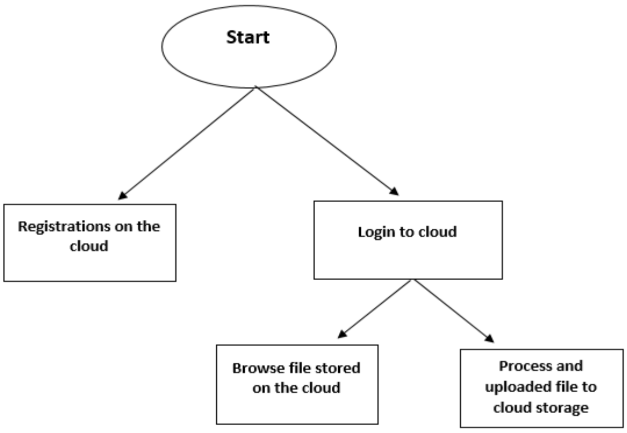
Start
Registrations on the cloud
Login to cloud
Browse file stored on the cloud
Process and uploaded file to cloud storage

Figure 1. General Work Flow Diagram of the Proposed System

This system implement on the google cloud using google app and firebase cloud messaging API. To use the services provided by the cloud system, first user must register on the cloud by entering the username and static password and then register your smartphone as a third party to complete the registration process; android mobile application design to confirm the account of user on the cloud and send/ receive notification from cloud server. To complete the Smartphone registration process, the user will enter the same user name and static password previously registered in the Cloud Storage Services. A phone application designed for this purpose will be used to search for the Cloud data base. When the user name and password are found, will send request to the fire base cloud messaging API (application programing interface) asked for registration and then the FCM will response with message of unique string (token) generated for particular user smart phone. This token will be store in the cloud database according to username and password to using it when send or receive notification on mobile. After token stored in the cloud database the user complete the process of registration and can login to cloud at any time and from anywhere by using his information. Figure 2. Explain the steps of registration process.

After complete the process of registering his account on the cloud storage and the Corresponding third party device, now can login to cloud. You must enter the previously registered user name and if valid System will generate the one time password using chaotic system. This chaotic system is non liner equation called duple sin chaotic equation that used to generate random number that cannot be predicted thus as a one-time password and will be expired after half an hour or one use. The duple sin equation is one of the important equations that used in security. It shown in equation 1.

$$\mathbf{Xn+1 = c2\ sin\ (\pi c1\ sin\ (\pi * Xn))} \qquad (1)$$

Equation 1: duple sin chaotic equation

The one time password that generated from the chaotic system will be send to the user on mobile then the user can used this received password on mobile application Combines with the static password that used in the registration as a password to login the cloud and using cloud storage to store his data, browses his file that stored on the cloud storage and downloading any file, Figure 3 explain the login operation.

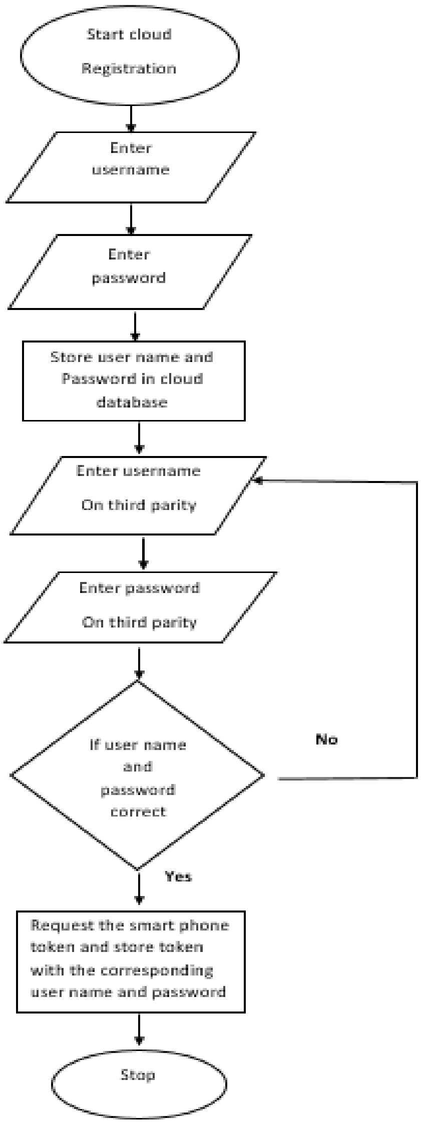

Figure 2. Registration Process

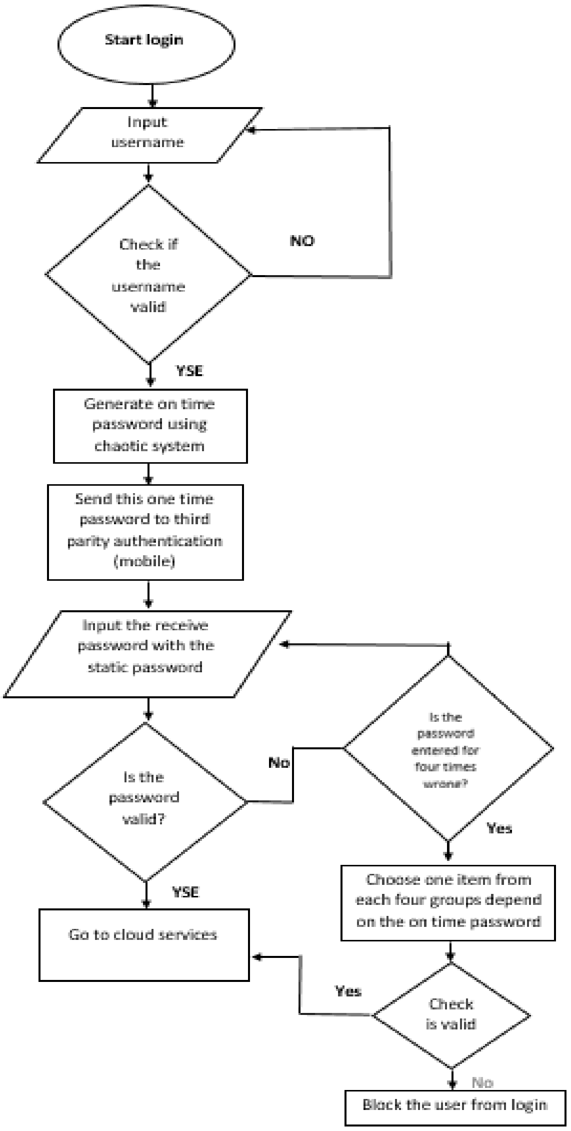

Figure 3. Login Process to Cloud Storage

When the user login to the cloud, he can use all the facilities provided by the system such as browses any file that are pre-stored in the google cloud storage and can download any file and read it and can upload any file to cloud storage.

User choses file to upload it to cloud storage and before storing the file will be encrypt using modified AES encryption algorithm as other level of security to secure sensitive data. The AES encryption algorithm is one of the most important Synchronic cryptographic algorithms, which is characterized by the speed of encryption and the difficulty of decoding the key encryption. The modified AES encryption algorithm used the expansion key method with double sin chaotic system to generating encryption key. Algorithm 1 explain expansion key method and algorithm 2 explain the modified AES encryption algorithm.

Algorithm (1): Expansion key algorithm

```
Input: key as an array of 32 word with 4 column and 8 row, NK=8
        Output: w as a two dimension key array
Begin:
        Step 1: for i = 1 to 8
        Begin
        Step 2: array r = (key[4 * i], key[4 * i + 1], key[4 * i + 2], key[4 * i + 3])
        Step 3: w[i] = r
        End
        Step 4: for i = 8 to 60
        Begin
Step 5: for t = 1 to 4
        Begin
Step 6: array temp[t] = w [i - 1] [t]
        End
Step 7: if (I mod 8=0)
        Begin
Step 8: shift row (temp)
Step 9: set t=1 to 4 do step 10
        Begin
Step 10: temp[t] = temp[t] AND rCon [i / 8][t]
End
Else
Begin
Step 11: if (NK > 6 && i mod Nk = 4)
Begin
Step 12: temp = s-box (temp)
Step 13: shift row (temp)
End
End
Step 14: h=1 to 4
Begin
Step 15: w[i][t] = w[i - Nk][t] AND temp[t]

End

End

End

End

Step 16: return (w)

        End.
```

```
Algorithm (2): Modified AES encryption algorithm
Input: w as a plan array with (256 bit) eight row and four column
Output: w as a cipher array with (256 bit) eight row and four column
Begin:
Step 1: Set I = 1
Step 2: Add Round Key generated by Double-Sine equation
$X_{n+1} = c2 \sin(\pi c1 \sin(\pi x_n))$ XOR with the result of algorithm 1
Step 3: While $I \le 13$
Begin
    Step 4:  Sub Bytes
    Byte by byte substitution with an S-box table
    Step 5: Shift Row
    Shifting one element to left depends upon the numbers of row
    Step 6: Mix Column
    Each column of the array is multiplied by a constant fixed mix column array
    Step 7: Add Round Key generated by Double-Sine equation
    $X_{n+1} = c2 \sin(\pi c1 \sin(\pi x_n))$ XOR with the generated by algorithm (1)
End
Step 8: Sub Bytes
Byte by byte substitution with an S-box table
Step 9: Shift Row
Shifting one element to right
Step 10: Add Round Key generated by Double-Sine equation
$X_{n+1} = c2 \sin(\pi c1 \sin(\pi x_n))$
End.
```

4. RESULT

4.1. Test Randomize

To test the randomize of the modifies AES encryption algorithms, we use Cryptool 1.4.30 software, Table 1 has the result of the five basic tests of the standard AES-256 bits compared with the modifies AES-256 bits encryption algorithm.

Table 1. Five Basic Test of AES and Modified AES Encryption Algorithm

Standard AES encryption algorithm randomness test											
File type	File Size	Frequency		Poker		Run test		Long run		Serial	
		Test result	Pass value	Test result	Pass value	Test result	Pass value	Test result	Pass value	Test result	Pass value
PDF	33 MB	2.29	3.84	-9.9	14.07	2.22	9.48	29	34	2.40	5.99
Png	9.61 MB	0.02	3.84	-4.14	14.07	10.18 fail	9.48	24	34	0.82	5.99
Mp4	5.03	1.74	3.84	-2.76	14.07	3.04	9.48	25	34	1.76	5.99
Mp3	11.9 MB	0.02	3.84	-3.36	14.07	3.76	9.48	26	34	1.68	5.99

Standard AES encryption algorithm randomness test											
File type	File Size	Frequency		Poker		Run test		Long run		Serial	
		Test result	Pass value	Test result	Pass value	Test result	Pass value	Test result	Pass value	Test result	Pass value
PDF	33 MB	0.06	3.84	-9.83	14.07	2.04	9.48	30	34	0.98	5.99
Png	9.61 MB	0.15	3.84	-4.64	14.07	7.86	9.48	25	34	0.89	5.99
Mp4	5.03 MB	0.60	3.84	-2.76	14.07	2.45	9.48	24	34	0.78	5.99

4.2. Cloud Storage Security Attack

The proposed system handled many security breaches such as insecure interface and API, The system does not contain any API and is not interleaved with any other system, it prevent Malicious Insiders due the users data stored in cloud storage in an encrypted format so that the Malicious Insiders cannot return the encrypted users data to original format. The develop system overcome the brute force attack and denial of service attack by following the method in case if the user entered the password wrong for more than four times the developed system will offer the user four groups of image and select from each group the image have number equal to the one time password that received on the mobile in the login step. The develop system overcome the SQL-injection attack by making tables for key words and check user input with reserved words.

4.3. Compare Propose System with Other System

Proposed method	One time password	Third parity	Encryption algorithm
Secure system to store privet data on cloud	One time password generated by chaotic system	Smart phone	Modified (AES) encryption algorithm with 256 bit
Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm	Not used	No used	Diffie-Hellman algorithm for key exchange. Digital signature is used for authentication. AES encryption algorithm is used to encrypt user's data.
Secured Cloud Architecture for Cloud Service Provider	Not used	No used	standard(AES) encryption algorithm
A New Framework for Cloud Storage Confidentiality to Ensure Information Security	Not used	Not used	Use Station-to-Station Key Agreement protocol for key exchange. SHA-1 for integrity of data server.(AES) encryption algorithm to encrypt user data

5. CONCLUSION

Cloud computing provide many services and uncounted benefit but the most important challenges in cloud computing and cloud storage are security. So this paper will provide secure system to store privet data in the cloud. These secure systems consist of two level of security. First level of security is secure login: in this layer the proposed system will generate the one time password by duple sin chaotic system to prevent unauthorized people to access sensitive data and third parity (smart phone) to prove a person's identity and to receive the one time password. The second layer of the proposed system is encryption in which data will be encrypted by using modified AES encryption algorithm before storing it in the cloud. The proposed system will overcome most type of attacker on cloud storage such as brute force attack and denial of service attack where the system prevent the attacker from block the service from legal user by using the group of images rather than blocked for some time to prevent the brute force attacker machines, also check the input information precisely to avoid SQL injection.

REFERENCE

[1] C. M. R. Da Silva, J. L. C. Da Silva, R. B. Rodrigues, G. M. M. Campos, L. M. Do Nascimento, V. C. Garcia. "Security threats in cloud computing models: Domains and proposals," *IEEE Int. Conf. Cloud Comput. CLOUD*, 2013: 383–389.

[2] T. K. Damenu, C. Balakrishna. "Cloud Security Risk Management: A Critical Review," *Next Gener. Mob. Appl. Serv. Technol. 2015 9th Int. Conf.*, 2015: 370–375,.

[3] M. Irfan, M. Usman, Y. Zhuang, S. Fong. "A Critical Review of Security Threats in Cloud Computing," *Comput. Bus. Intell. (ISCBI), 2015 3rd Int. Symp.*, 2015: 105–111,.

[4] J. Domzal. "*Securing the cloud: Cloud computer security techniques and tactics" (Winkler, V.; 2011) [*Book *reviews]*, 2011; 49(9).

[5] Cloud Security Alliance. "Top Threats to Cloud Computing," *Security*, no. March, 2010: 1–14.

[6] A. Hendre, K. P. Joshi. "A Semantic Approach to Cloud Security and Compliance," *Proc. - 2015 IEEE 8th* Int. *Conf. Cloud Comput. CLOUD 2015*, 2015: 1081–1084.

[7] C. Standards, C. Council. "Security for Cloud Computing Ten Steps to Ensure Success," 2015.

[8] S. S. Manikandasaran."Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage," *IRACST - Int. J. Comput. Sci. Inf. Technol. Secur. (IJCSITS)*, 2016; 6: 498–503.