International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

# Symmetric Hash Encryption Image as Key (SHEIK)

**Sheik Khadar Ahmad Mnoj, D.Lalitha Bhaskari**

***Abstract*: Cloud storage model have become a widely accepted solution for the growing demand of online storage and remote accessing. Cloud service provider (CSP) provides the online storage facility for the cloud customer (CC) as per pay-by-use model. Data security still remains a threat for the CC to have a complete trust on the technology. The existing symmetric key algorithms to some extent have been successful in providing the confidentiality of the data. The main issue in implementing the algorithm is sharing of the key, if the key is known to others the security of the data is exploited. This paper tries to sort out the problem by making image as a key for the algorithm. The CC can perform the encryption before uploading the data to have the control of the process. The selection of the algorithm decides the key length to be extracted from the image making the method more secure and reliable for the CC. The experimental results have shown that the proposed Symmetric Hash Encryption Image as Key(SHEIK) method works satisfactorily for encrypting and decrypting the data efficiently.***

***Keywords: Cloud storage, Cloud customer (CC), Cloud service provider (CSP), Data security, Encryption algorithms, Key sharing.***

## I. INTRODUCTION

In this digitized world there is an emerging need for the data to be online and readily available globally for accessing it for the purpose of various business and personal requirements. The cloud storage model a service of cloud computing have supported the demand. The cloud storage services are offered to the clients by the service providers and are charged as per their usage. The CC found this model feasible both economically and technically. The recent surveys have shown that there is an increase in the number of cloud subscription. Security and privacy are the major concerns for the cloud computing since the advent of the cloud technology.

Data security is considered as most important factor to be dealt with before becoming the CC. Another major drawback in hosting the data into cloud is that the CC will possess no control over the data after it has been deployed in to the cloud servers. To enhance the data security the CSP have implemented the cryptography technology. The cryptography is a mechanism where the original data known as Plain text (Pt) is converted to a altered format known as Cipher text (Ct) such that it's meaning is not known until it gets decrypted.

The recent issues of data theft and cyber frauds have made the CC to doubt on the credibility of the CSP. The trust between the CC and CSP can never be accomplished as there is no permanent solution for the security and privacy. The CC always tries to protect the data in all possible manners he could. The CC with the awareness of technology sometimes performs encryption mechanisms before uploading the data to CSP. The insider attack which no CSP can avoid does add a notable entry in the list of security attacks.

On the other hand, to retain trust the CSP invests a huge amount in providing security solutions for the attacks. The CSP will always look and seek out various security aspects and installs various security tools, employ security personnel will eventually minimize the profit.

The CSP always rely on the encryption algorithms for the security of data. Symmetric encryption algorithms are considered to be more efficient and fast for encryption. The algorithm uses a key for encryption and the same key is used for decryption. The mostly used algorithms like 3DES, Blowfish, AES are known for their tolerance for various security attacks. The algorithms are strong until and unless the key is protected and kept secret. If the key is revealed then the confidentiality of the data is no more guarded. The key sharing is a major task in utilizing these algorithms.

In this paper, a methodology Symmetric Hash Encryption Image as Key (SHEIK) have been designed for the symmetric algorithms to have an image as key rather than any other text or binary values. The essential part of the SHEIK method is the flexibility of key sharing. This method works well not only in having a strong key but also keeping it secure and for the mechanism.

## II. LITERATURE REVIEW

The Cryptography is broadly categorized to three types basing on the keys and their functionalities. They are given below in figure 1.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
**Sheik Khadar Ahmad Mnoj,** Research Scholar, Department of Computer Science and Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, India, Email:skamanoj@gmail.com.
**D Lalitha Bhaskari,** Professor, partment, Department of Computer Science and Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, India, Email:lalithbhaskari@yahoo.co.in.

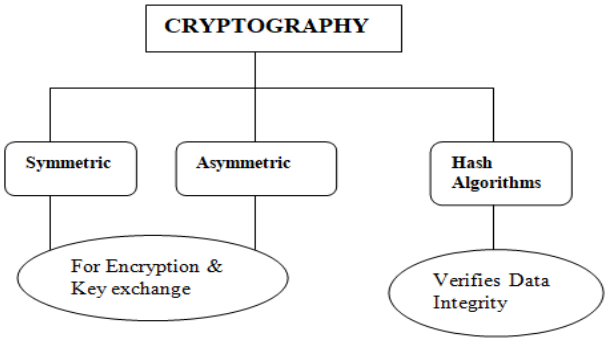


**Figure 1: Overview of Cryptography**

The algorithms work mainly on two principle methods of altering the given Pt. They are

**Substitution:** Replacing the given Pt with the predefined symbols for generating the Ct.

**Transposition:** Making the contents of the Pt to be permuted to give the Ct.

The above said symmetric and asymmetric algorithms work on these two principles with the involvement of key for producing the Ct. These algorithms can further divided into two types basing on the number of bits converted to Ct. They are:

**Block Cipher:** Here the number of bits is fixed and are kept in blocks if the number is not matched then they are padded with additional bits for making them equal to the block.

**Stream Cipher:** The Number of bits is not fixed and bits are encrypted as a stream of bits.

The Symmetric key cryptography involves a single key to be shared between the sender and the receiver. These algorithms are most time efficient and are frequently used in encryption. The mostly used encryption algorithms in cloud storage are: 3DES, AES, Blowfish, and RC6.

The Asymmetric key cryptography involves two keys one for encryption and the other for decryption. They take much more time for the cryptographic process and are preferred less. They are used for digital signatures a sort of integrity checking. The most popular are RSA, Diffie Hellman.

The Hash algorithms when supplied with Pt they produce a fixed size message digest (MD) and is sent to the receiver mostly with the message itself. The receiver will use the same hash algorithm on the message and compares the generated Md with the received Md if both are equal then he is assured that the message is not modified. If not then he confirms that the integrity of data is lost. The SHA-512, MD5 are some of the hash algorithms.

In this paper, symmetric algorithms and hash algorithms are selected to implement the proposed SHEIK .

The main drawback in breaking the DES is the Key length which was short and then the length of the was increased [2]. To make DES strong extension of DES known as 3DES was proposed which involves 2 or 3 keys [3]. The DES execution is faster than 3DES but in security aspect 3DES is considered more powerful.

Blowfish has variable key length and varies from 32 bits to 448 bits [14] and is also considered more secure.

The AES was proposed to execute faster than 3DES and it also has 3 key variants 128, 192, 256 and no of rounds are depend on the selection of the key[1][3].

The above said symmetric algorithms can only be compromised if someone gains the key. To share the key between the sender and the receiver steganography (hiding message in image) is being implemented [17]. The image is shared in a secured manner and the key is generated from the image [18].

From the above, it can be concluded that length of the key and security of key plays a vital role in shielding the Pt. If image is used as a tool of sharing the message there is a possibility that the data loss during transmission results in incorrect key extraction. To overcome the barrier the SHEIK method uses hash algorithm to verify the corre3ctness of the Key.

## III. PROPOSED SHEIK METHOD

The proposed Symmetric Hash Encryption Image as Key (SHEIK) focuses on a simple, flexible and secure key sharing. The SHEIK method is to be performed at the CC, the SHEIK method to be executed requires three things.

i. The Image which is used as key.
ii. The Symmetric algorithm and
iii. The Hash algorithm.

All the above three are selected by the CC which gives the control of the encryption mechanism to the CC.

The steps in the encryption process are given below

- The SHEIK method converts the image into binary values and the subset of them is selected as Key.
- The Key bits are fed to the hash algorithm and the generated Message Digest (MD) is retained at CC.
- The Message is converted to ASCII values and the subset of them is taken for encryption basing on the symmetric algorithm.
- The Ct thus generated is stored in the cloud.

The Md is not stored in the cloud and is sent to the receiver just before informing about the Key image. The overall encryption procedure is given in the following algorithm1.

// **Input**: Image and Message.

// **Output**: Cipher Text and Message Digest

**Algorithm 1: SHEIK Encryption Procedure**

1. Read the Image (I) and convert it into binary values and store them in Matrix $M_I$.
2. Take a subset of the binary values basing on the algorithm key size and store it in K.
   (For the size k of Symmetric algorithm (SA) read from $M_I$ and store them in K until size of(K)=k)
3. Calculate the MD of K and store it in M.
3. Read Message and covert them to ASCII values and store them in Matrix $M_T$.
4. Take a subset of the $M_T$ basing on the algorithm block size and store it in P.
   (For the size p of Symmetric algorithm (SA) read from $M_T$ and store them in P until size of(P)=p)
5. Perform encryption

on M with K store the cipher text in C.
i.e C=E(M,K);
6. Upload C in cloud.

The above algorithm is illustrated in figure 2. The MD of the key image is verified before downloading the C from cloud. If the verification is true then the decryption procedure is initiated or else CC will be asked to resend the key image again.

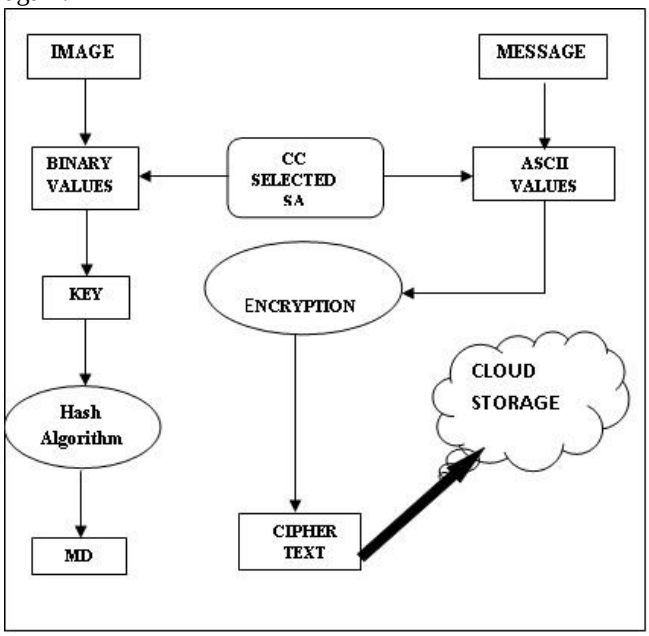


**Figure 2: SHEIK Encryption procedure.**

At the receiver side once the image and the MD is sent by the CC. The receiver will verify the integrity of the Key and if it is success then the Ct is downloaded from the cloud and then decryption is performed. The procedure is presented in algorithm2.

// **Input**: Image, M(MD of K of image).
// **Output**: Message

**Algorithm 2: SHEIK Decryption Procedure**

1. Read the Image (I) and convert it into binary values and store them in Matrix $M_I$.
2. Take a subset of the binary values basing on the algorithm key size and store it in K.
   (For the size k of Symmetric algorithm (SA) read from $M_I$ and store them in K until size of(K)=k)
3. Calculate MD and Verify with M.
   IF SUCCESS download C from cloud.
   ELSE ask CC to resend image
   END IF.
4. Perform decryption on C with K store in H.
   i.e H=D(C,K);

**Illustration with an example**

Take an image of your own collection or download it from web. Here, a picture is downloaded from Web shown in fig 3.

**Figure 3. Sample image,lena [7]**

The corresponding binary values are stored in Matrix $M_I$ as given below. (Only a portion of the values are taken for the space constraint)

**$M_I$=**

Let the CC select an algorithm which requires the Key length to be a 64 bit. Then the bits from $\mathbf{M_I}$ are selected by using the following function.

K= f($\mathbf{M_I}$ 64)

```
11100000100000000011111100000001111111
11100000100000000111111100000001111111
01100000100000001111111100000011111111
11100001000000001110111100000011111111
00111000110000000110000110000000111111
00111000100000001110010110000001111111
00111000000000001011111111000001111111
00011000000000010011111111000001111111
00011000000000000011101110000011111111
00111000000000100011101100000011111111
00111000000000000011111110000011111111
00111000000010000001001100000111111111
```

[ **f($M_I$,n)=** if n is a perfect square
Let r=1;
Until r= √ n
for each row r in M1 take √ n symbols and store in K
else
Let r=0;
For each row take individual element r until r=n;]

**K=**

```
11100000
11100000
01100000
11100001
00111000
00111000
00111000
```

**HashMD(MD5)=** 75a1733f1786657eb06dce3da10fb

The Message is converted to ASCII values and stored in $\mathbf{M_T}$

Message= ”Hello everyone”

$M_T$=

| | | | |
|---|---|---|---|
| 01001000 | 01100101 | 01101100 | 01101100 |
| 01101111 | 00100000 | 01100101 | 01110110 |
| 01100101 | | | 01110010 |

Let the CC select an algorithm which requires the Text length to be a 64 bit. Then the bits from are selected by using the a function to generate P.

**P=j ($M_T$, n**

**P=**

| |
|---|
| 01001000 |
| 01100101 |
| 01101100 |
| 01101100 |
| 01101111 |
| 00100000 |
| 01100101 |
| 01110110 |

Then, both the P and K are sent to the encryption algorithm to generate a cipher text, C.

**C=**

| |
|---|
| tcPioNTvWFS/ZYqFv9Fu9L9K |
| JYbP9DkaBUjRRqjrTgxLnE3E |
| 9KWId1h/AHKAdx8UtCPDuB |
| VdbRcStdfVn+2bS4EaqhE8sPF |
| LqAfG+FxT5+EZzBrP0i6+lKv |
| BBQeQN7c/ |

The Cipher above produced is uploaded into the cloud. The sharing of the MD and the image through which the key is generated is the sole responsibility of the CC.

## IV. RESULTS AND DISCUSSION

The implementations have been performed on java1.8 platform on Intel core i7@3.40Ghz processor with 8GB RAM and 64bit windows 7 operating system. The main advantage is SHEIK method is that it makes the insider attack and brute force attack weak. Even though there is a overhead of performing SHEIK the security aspect will make the little work negligible. The recent advantages of the computing power and the decline in the primary storages will boost up the CC to adopt this method.

The following table1 shows the additional time taken for converting the images to Keys and table2 shows the time duration for text to ACII values.

**Table 1: Time taken for executing the images.**

| Image Size | Time taken to convert to binary values in seconds. | Time taken to convert to Key in seconds. |
|---|---|---|
| **10KB** | ***0.248*** | ***0.020*** |
| **20 KB** | ***0.512*** | **0.112** |
| **50 KB** | ***0.927*** | **0.266** |
| **100 KB** | ***1.24*** | **0.532** |
| **200 KB** | ***2.48*** | **1.75** |

From the above table, it is evident that it is not a huge time taken process and the lapse can be overlooked keeping the security aspect as primary importance.

| Text Size | Time taken to convert to ASCII values in seconds. | Time taken to Select block size in seconds. |
|---|---|---|
| **5KB** | ***0.098*** | ***0.018*** |
| **10 KB** | ***0.226*** | **0.297** |
| **50 KB** | ***0.453*** | **0.655** |
| **100 KB** | ***0.798*** | **0.982** |

The above table shows that the time for image processing is a little bit higher than to preprocess the text messages for the SHEIK method.

- The advantages of SHEIK method over the existing encryption mechanisms can be written as below:
- SHEIK method is applied at off-line makes it tolerant to the cyber-attacks and the throughput can be maximized in standalone systems compared to network connected sysem.
- The CC can be share the key and MD just before decryption to the receiver making the feasible key sharing.
- The image is chosen randomly makes the possibility of guessing the key more difficult for the insider attacks.
- The CSP can now have cut in the security investments and can maximize the revenue.

## V. CONCLUSION

The objective of the proposed SHEIK method is to bridge the gap between the CC and CSP by providing a mechanism of enhancing security to the data. The model has brought together the image and the text for encrypting the data in such a way that key confidentiality shouldn't be a load for the users. The above algorithm showed desirable results to ensure trust in the cloud storage. Even though, the combination of off-line and online looks a tedious job, but the outcome of this makes the method acceptable.

The SHEIK can be extended to have audio and videos as keys in near future as the processor speeds are now increasing in exponential manner. The major limitation for this algorithm is that if the CC is not able to implement then the CSP have to again given back the control of encryption..

## REFERENCES


1. M. Umaparvathi and D.K. Varughese, "Evaluation of symmetric encryption algorithms for MANETs," IEEE International Conference on Computational Intelligence and Computing Research, 2010, pp. 1-3
2. S.R. Masadeh, S. Aljawarneh, N. Turab, and A. M. Abuerrub, "A comparison of data encryption algorithms with the proposed algorithm: Wireless security," Sixth International Conference on Networked Computing and Advanced Information Management, 2010, pp. 341-345
3. D.S.A. Elminaam, H. M. Abdual-Kader, and M.M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," International Journal of Network Security, vol. 10, pp 216-222, 2010
4. T.S. Barhoom, Z.M. Abusilimiyeh, "A Novel Cryptography Method Based on Image for Key Generation", IEEE Proceedings on the Palestinian International Conference on Information and Communication Technology, 2013, pp. 71-76.
5. A. Sahu, Y. Bahendwar, S. Verma, P. Verma, "Proposed Method of Cryptographic Key Generation for securing Digital Image". International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2(10), 2012, pp. 285-291.
6. A Survey Paper on Cloud Storage Auditing with Key Exposure Resistance - Sneha Singha , S. D. Satav - International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611,2014
7. https://www.bing.com/images/search?q=image%20processing%20lena&qs=n&form=QBIRMH&sp=-1&pq=image%20processing%20lena&sc=2-21&sk=&cvid=E3147040D2514B81B1740B08FDC34783

8. C. Wang, K. Ren, W. Lou, and J. Li, “Toward Publicly Auditable Secure Cloud Data Storage Services,” IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
9. Wentao Liu, "Research on cloud computing security problem and strategy", IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 1216-1219
10. Prerna Mahajan, Abhishek Sachdeva, “A Study of Encryption Algorithms AES, DES and RSA for Security”, Global Journal of Computer Science and Technology Network, Web & Security, Vol.13, Iss. 15,Vol. 1, 2013.
11. Chun-I Fan S-YH (2013) Controllable privacy preserving search based on symmetric predicate encryption in cloud storage. Future Gener Comput Syst 29:1716–1724

## AUTHORS PROFILE

**Sheik Khadar Ahmad Mnoj,** is a research scholar in the department of Computer Science and Systems Engineering, AUCE(A), Andhra University, Visakhapatnam He have completed his M.Tech from Pydah Engineering College, Visakhapatnam. He has 6 years of  of teaching experience and his research interests are in the fields of Cloud security, Encryption mechanisms, Image processing  and Artificial Intelligence. He has published his work in international journals and conferences.

**Prof. D. Lalitha Bhaskari** is working as professor in the department of Computer Science & Systems Engineering(CS&SE), AUCE(A), Andhra University, Visakhapatnam. She has 20 years of teaching experience and her research areas include cryptography & Network Security, Computer Vision, Cyber Forensics & Deep learning. She has nearly 50 papers in reputed international journals and 32 papers in proceedings of international conferences. She has done international consultancy works related to deep learning with respect tp image segmentation .She is a life member of a few reputed professional bodies. She is a receipient of “Young Engineers” award by IEI, India during the year 2009.