ISSN (e): 2250 – 3005 || Volume, 08 || Issue,10|| October – 2018 ||
International Journal of Computational Engineering Research (IJCER)

Secure Migration of Data in Cloud Using Enhanced AES Algorithm

[1]Hitesh Marwaha, [2]Rajeshwar Singh,
[1]*Research Scholar, IKG Punjab Technical University, Jalandhar, Punjab, India*
[2]*Director, Doaba Khalsa Trust Group of Institutions, SBS Nagar, Punjab, India*
Corresponding Author: Hitesh Marwaha

ABSTRACT:
Cloud computing is an emerging internet based computing technology. Increased demand of computing resources has raised the need to outsource the resources and made cloud most enticing technology nowadays. As it is internet based technology so the challenges faced by internet based technologies are the major challenges of cloud computing. Security and privacy are major challenges due to which organizations are not migrating data to cloud with full confidence. 128 bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. Due to some drawbacks of AES several algorithm has tried to modify the static nature of S-box. An attempt has been made in this paper to modify AES. This paper highlights security threats in cloud and proposed an enhanced AES algorithm to migrate data to cloud securely.
KEYWORDS: Cloud Computing, CSP, AES, Cryptography, MAC,S-Box,

---

Date of Submission: 15-12-2018 Date of acceptance: 31-12-2018

I. INTRODUCTION

Sharing or transferring data from one end to another is backbone of present information technology era Cloud computing is a network based technology based upon pay per usage model and most enticing technology these days. Cloud computing provides broad network access, storage space, computation resources, user and applications etc.[1] Due to quick growth in technologies more and more service providers and customers migrating towards cloud environment. As security is one of the important aspects that are considered in network based technologies, so same is the concern that is the hindrance in the wide acceptance of cloud computing. Securely transferring of data need a mechanism to encrypt or ciphering the data. The data which is stored in the cloud is not much secure according to the user's point of view. Cryptography is considered as one of the solutions for the data security. [2]

1.1 Major Security Concerns in Cloud:

- Account or service hijacking: An account can be hijacked due to weak credentials. If user's credential's are accessed by malicious user, he can access sensitive data in cloud , manipulate data.[3]
- Malicious insiders: Internal attacks by the malicious employee of the CSP can do more damage to the data than the external attackers. A malicious employee from the company could easily access the detail of all customers or contacts and misuse the same when he is employed by a competitor.[4]
- Data Loss: Data loss unlike a computer bug occurs due to deliberately or not deliberately changed from its original or correct form to erroneous form. Data loss can be systematic or random, and even a small change can leave a file useless. [5]
- Insecure API: Application Programming Interface (API) is a set of rules a define the communication between software applications through internet. Cloud APIs are used at all the IaaS,PaaS,SaaS service levels to communicate with other services Cloud service providers usually offer their APIs to third party to give services to customers. Weak set of APIs could result in many security and privacy issues in cloud. Weak APIs enables the third party having access to security keys and significant information in cloud. [6]
- Denial of Service: Denial of Service (DOS) attacks are done to prevent the genuine users from accessing cloud network, storage, data, and other services. DOS causes delay in cloud operations as well as cloud stops to respond to other users and services.[7]

II. CRYPTOGRAPHY

Cryptography is used to defend information content communicated over a network from being accessed by opponent. This is attained by transforming (encrypting) plaintext before
transformation (decryption). Important factors that comprise in cryptography are of some basic terms[8]
1. Confidentiality:- This means privacy and Assurance of data
2. Authentication: - Data should be reached to claimed user only.
3. Integrity: - This means data should not disturbed by an unauthenticated person.
4. Non-repudiation:- Means denial protection.
5. Access Control:-Prevents misuse of resource.
6. Availability: Data should be available with high performance, non-erasure.

They can be divided into Symmetric and Asymmetric key cryptography. Symmetric key cryptography is a form of encryption that uses the same key to both encrypt and decrypt data.[9] The key should be distributed before transmission between two parties. Key is the backbone of encryption and decryption . The use of a weak key in the algorithm can decrypt the data easily.The size of the key determines the strength of Symmetric key encryption.[10] Symmetric algorithms are of two types: block ciphers and stream ciphers. The block ciphers are operating on data in groups or blocks. .Examples are of Data Encryption Standard (DES) Advanced Encryption Standard (AES) and Blowfish. Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm.

2.1 DES

DES is very generally exploited symmetric key algorithm. It was developed in the early 1970s at IBM. However DES was very popular at that time and was promptly implemented for non-digital media, such as voice-grade public telephone lines and the banking industry as a wholesale banking standard [11] but today's numerous techniques are established that have proved this algorithm unsecured [12]. In DES algorithms, a block cipher is of 64 bits [13] and key used is of 56 bits out of 64 bits of key is a utilized rest of 8 bits is padded. In a block cipher data block involving plain text is encrypted to create a cipher block through a mixture of diffusion and confusion. Cipher block so created is then passed through 16 rounds, earlier passing through these 16 rounds the 64 bits of data is separated into 32 bits. After separating the data into 32 bits, F-function (Feistel function) is applied. F-function involves of three processes substitution, permutation and key mixing. The function o/p is applied with another half of the data involves XOR gate alternate crossing of data [14]. After doing, 16 such rounds cipher's text is produced or encryption of data is complete. To decrypt the data inverse operation is done. The drawback of DES is that key used in DES is very small and its security can be cracked easily, and DES works fast on hardware only and woks slowly on software. As

2.1 AES

AES algorithm is currently the standard block-cipher algorithm that has replaced the Data Encryption Standard (DES) algorithm. [15] AES is used is used for secure transmission of user's
authorized data in encrypted format. AES takes into consideration three distinct key lengths: 128,192 or 256 bits. [16]

For encryption, each round consists of the following four steps:
1. Substitute bytes
2. Shift rows
3. Mix columns
4. Add Round key
For decryption, each round consists of the following four steps:
1. Inverse shift rows
2. Inverse substitute bytes
3. Add Round key
4. Inverse mix columns.

Step 1: Substitute bytes:
This stage (known as Sub Bytes) is simply a table lookup using a 16×16 matrix of byte values called an s-box. This matrix consists of all the possible combinations of an 8 bit sequence (28 = 16 × 16 = 256). However, the s-box is not just a random permutation of these values and there is a well defined method for creating the s-box tables. The matrix that gets operated upon throughout the encryption is known as state. In a particular round each byte is mapped into a new byte in the following way:

The leftmost nibble of the byte is used to specify a particular row of the s-box and the rightmost nibble specifies a column. The Inverse substitute byte transformation (known as InvSubBytes) makes use of an inverse s-box.
Step 2:Shift Rows:
The output of substitute byte transformation is input to shift rows transformation which consists of rotation of each byte of the state array in the order of a row of data matrix (rotation of row, byte positions is done in this step). Each byte of the first row remains unaltered. Every byte in second row is rotate over one byte to the left position. Correspondingly, the third and fourth rows are also rotated left by two and three-byte position. The corresponding shifting rows step used throughout decipherment is named Inverse Shift rows.
Step 3: Mix columns:
Mix columns perform operation on the state array obtained from Shift Rows column by column and each column is multiplied with row of a fixed matrix. This progression takes four bytes as an input and produces outputs of four bytes (every input byte influences the output bytes). The four numbers of state arrays of first column are modulo multiplied in Rijandeal's Galios Filed (GF) by a given matrix. In AES Mix column step, along with shift rows are primary source for providing complete diffusion to the cipher produced. The corresponding Mix column step used throughout decipherment is named Inverse Mix columns.
Step 4: Add Round key:
In the add round key step, the Round key which is generated using Rijindael's key schedule is combined with the new state obtained from Mix columns transformation state. The round key is added by consolidating every kind of the state array using bitwise XOR operations. The actual 'encryption' is performed in the add round key, when each byte of state is XORed with the round key to produce final cipher text.

III. RELATED WORK

In this paper [18] modified AES which uses MAC address is proposed to transfer data in cloud. MAC Address enhances the randomness of the AES processes as it is different in each computer. Finally it is concluded that attacker could not break the encrypted message easily although primary key is known to them.
In this paper[19] the process of transferring the files to the cloud and retrieving the files from the cloud was accomplished by symmetric and asymmetric encryption respectively. The RSA encryption provides intricacy for hackers as well as minimizes the time of information transmission by using AES encryption method. Although combination of asymmetric and symmetric encryption techniques can achieve the assurances of cloud data security yet the double encryption and decryption process for each files cause system overhead.
This paper [20] highlights the various existing security issues in cloud computing environment and proposed a new method for securing cloud data. The 128 bit AES encryption is proposed for granting the basic information security measures like confidentiality, authenticity and access control to data. Although proposed method provides the cloud data security yet it is observed that there is extreme increase in delay with increase in file size.
In this paper[21] to enhance the security to maintain confidential of data to be stored in cloud AES is proposed. It is also concluded that the strength of AES encryption algorithm depends upon size and format of files to be transferred. Initially it is suggested that for large data size file 128 bits key encryption, for medium data 192bits key and for small data 256 bits key should be used. Representing the size of data variations after encryption 14 no of iterations. Finally it is concluded that encryption with 256 bits key should be done based on the data format than the size of the data.
In this paper[22], to provide privacy and security to the data to be transmitted as well as data stored on cloud, a client side encryption and decryption technique using single secret key is proposed. Finally after analyzing various techniques it was concluded that AES encryption and decryption method guarantees the security and privacy in the cloud.
In this paper [23] an innovative Block key generation algorithm with an addition of dynamic S-box generation algorithm is proposed. It can be applied to AES-128 variant. All of the block keys are generated prior to the initiation of Advanced Encryption Standard (AES), this property makes it possible to encrypt each block of plain text in parallel and hide plain text patterns. The proposed algorithm ensures security and privacy of data but its operational complexity is a little higher than AES.

IV. PROPOSED WORK

4.1 Secure MAC Key Generation

Secure MAC Key Generation algorithm (SMKG): In proposed technique to generate unpredictable key in AES a secure MAC key generation algorithm is used.

Algorithm I (128 bits)

This algorithm is used to create more secure key for AES algorithm.

1. X: = 128 bit private key.
2. Let M: = MAC address of computer from where data is to be migrated.
3. Convert the MAC address into 128 bits by using SHA-128.Let 128 MAC is assigned to variable M1
4. K1 = X⊕M1 [Apply XOR on secret key and 128 bit MAC address.]
5. The value so generated K1 is passed through SHA-256 algorithm. Let it be stored in SK.
6. Trimmed output creator converts the value generated by SHA 256 (SK) into 128 bits.

It generates non identical block keys from the user provided 128 bit secret key to encrypt every block of plain text. Exclusive OR operation is applied on the secret key and the MAC address of the computer. Secured hash algorithm SHA 128 is applied to convert MAC address into 128 bits. Then
the transformed key so generated acts as the input for SHA-256 algorithm and finally a Trimmed output creator creates 128 bit, block key to be used in encryption or decryption. The process of generating block keys from the secret key is depicted in Figure I,II, and III respectively.

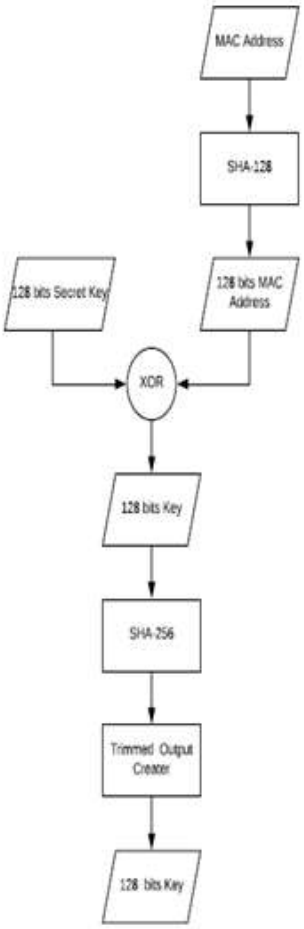

Figure I

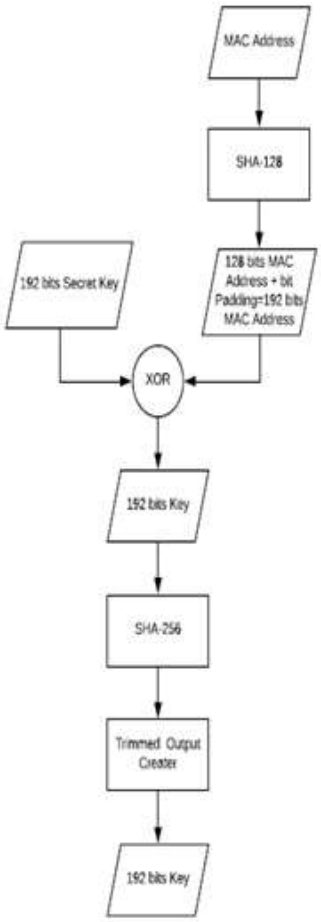

Figure II

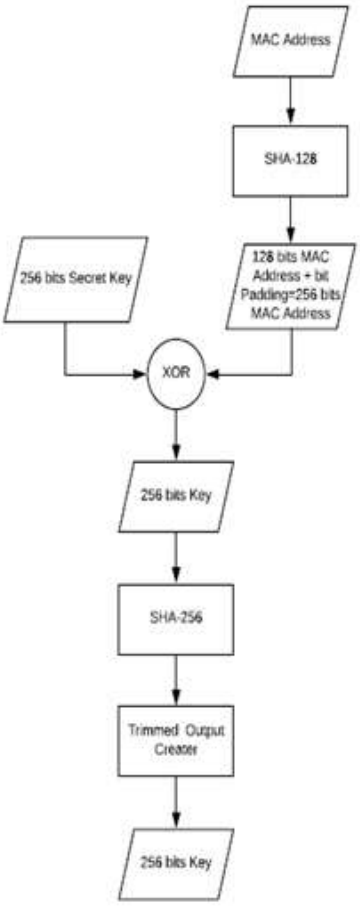

Figure III

Trimmed Output Creator: Trimmed output creator is used to generate the key of appropriate length. The output generated by SHA-256 is of 256 bits. As in AES there are three variants of key size 128 bits,192 bits and 256 bits. So in three cases it perform differently:

128 bits Variant: The 256 bit output generated by SHA-256 is divided into two parts and then XOR is applied on both parts and final 128 bits output is generated.

192 bit Variant: The 256 bits output generated by SHA-256 is divided into two parts of 128 bits each, then 128 bits are again divided into two parts of 64 bits each. Then XOR is applied on two parts and combined in order to produce 192 bits output. 256 bit

variant: In this case no further operation is applied on 256 bits output generated by SHA-256.

4. 2 Enhance AES:

AES proposed in this paper is modification over primitive AES in two manners, first key generation process (as explained in algorithm I) and use of key dependent S – Box (Dynamic S-Box) instead of static S-box.

The detailed process is explained in figure IV

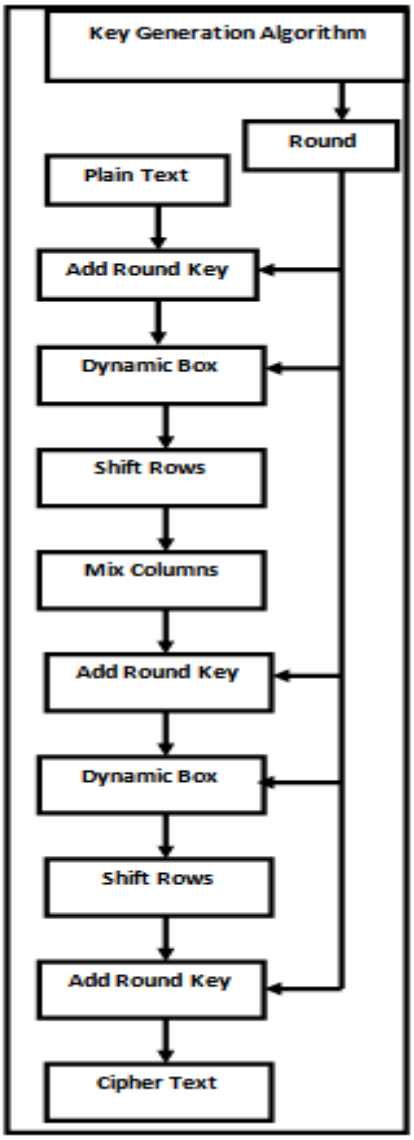

Figure IV

4.3 Key Dependant S-Box Generation (Dynamic S-Box)

Advanced Encryption standard uses static S-box for encryption generated by calculating multiple Inverse of each byte ranging between 00 to FF in hexadecimal form. While S-box used in decryption is inverse of that used

in encryption. . In proposed technique S box are dynamic and generated by applying aforementioned round key generation algorithm.
The process of encryption starts with the generation of dynamic S box which include following three steps [24]

- Generate round key
- Apply XOR operation on every byte of round key.
- The value so obtained is used for left circular rotation or right circular rotation of static S-Box.

For example Let A1 to A16 is 16 bytes key.
A1⊕A2⊕A3⊕A4⊕A5⊕A6⊕A7⊕A8⊕A9cA10⊕A11⊕A12⊕A13⊕A14⊕A15⊕A16
Let us suppose after application of key generation algorithm following key in hexadecimal form is generated

59	AF	5a	E3	87	F6	DE	98
3C	E9	01	C7	B9	18	F8	F1

After application of XOR operation on the round key so obtained, resultant value generated is 3C in hexadecimal or 60 in decimal. Now the decimal value 60 is used to cyclically rotate static S-box to the left by 60 bytes. The dynamic S Box so generated by cyclically left rotation is depicted in figure V.

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8	ba	78	25	2e
10	1c	a6	b4	c6	e8	Dd	74	1f	4b	bd	8b	8a	70	3e	b5	66
20	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e	e1	f8	98	11
30	69	d9	8e	94	9b	1e	87	e9	ce	55	28	Df	8c	a1	89	0d
40	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	Cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	Ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b
c0	fe	d7	ab	76	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af
d0	9c	a4	72	c0	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1
e0	71	d8	31	15	4	c7	23	c3	18	96	5	9a	7	12	80	e2
f0	eb	27	b2	75	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3

Figure V

V. ADVANTAGES OF PROPOSED TECHNIQUE:

Advanced Encryption Standard (AES) is one of the cryptographic methods that currently considered safe and strong enough. Although AES is most widely accepted symmetric key technique for security of data yet brute force attacks could also break AES quickly if the key used is weak. In proposed technique use of MAC address increases the randomness of the AES process because it is different for each computer. Other major drawback of AES is use of static S box; the same is rectified by use of dynamic S box in proposed technique. The use dynamic S-box eradicates any possibility of cryptanalysis and makes the proposed system more secure.

VI. COMPARISON OF OPERATIONAL COMPLEXITY:

There are two major criterions complexity and time to measure the performance of an algorithm.
The proposed system is more complex than AES due to major factors such as use of MAC address while key generation and use of key dependant S- box every time. However the proposed algorithm rule out the drawback the Enhanced AES use of MAC address [18] and Enhance AES using novel block key dependent S-Box[23] by not using permutation function that increases number of iteration while generating key so the system were more

complex. The proposed system is less complex the above stated enhanced AES algorithms but more complex than AES. The proposed system overcomes the drawback of AES.

VII. CONCLUSION

The organization can get real benefits of the most enticing technology of current information technology if CSP provides the guarantee of security of their sensitive data from malicious users or unauthorized access. The proposed enhanced version of AES is an alternative to existing symmetric cryptography algorithm. Attackers probably could not break the encrypted message easily even they know the primary key. The proposed algorithm is to some extent more complex and requires more execution time as compared to AES. However for security and privacy of sensitive data the little more complexity and execution time can be compromised. In future work can be done to reduce the operational complexity of proposed algorithm.

REFERENCES

[1]. Shimbre, Nivedita, and Priya Deshpande. "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm." Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on. IEEE, 2015.

[2]. Raj, Gaurav, Ram Charan Kesireddi, and Shruti Gupta. "Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015

[3]. Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of internet services and applications4.1 (2013): 5.

[4]. https://securitycommunity.tcs.com/infosecsoapbox/articles/2017/02/14/10-major-security-threats-cloud-computing

[5]. https://www.makeuseof.com/tag/data-corruption-prevent/

[6]. Kazim, Muhammad, and Shao Ying Zhu. "A survey on top security threats in cloud computing." International Journal of Advanced Computer Science and Applications (IJACSA)(2015).

[7]. https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[8]. Symmmetric Key Based Cryptographic Techniques : A Recent Survey Sonawane Yogesh Kailas1 , Vijay Kumar Verma2 1 M.Tech IV Sem. Lord Krishna College of Technology Indore 2 Asst. Professor (CSE) Lord Krishna College of Technology Indore

[9]. Agrawal, Himani, and Monisha Sharma. "Implementation and analysis of various symmetric cryptosystems." Indian Journal of science and Technology 3.12 (2010): 1173-1176.

[10]. Mandal, Pratap Chandra. "Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish." International Journal of Global Research in Computer Science (UGC Approved Journal) 3.8 (2012): 67-70.

[11]. Grabbe, J. Orlin. "The DES algorithm illustrated." Laissez Faire city times 2.28 (1992): 12-15.

[12]. Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering 1.2 (2011): 6-12.

[13]. Jain, Neha, and Gurpreet Kaur. "Implementing des algorithm in cloud for data security." VSRD International Journal of Computer Science & Information Technology 2.4 (2012): 316-321.

[14]. Pansotra, Er Ashima, and Er Simar Preet Singh. "Cloud security algorithms." International Journal of Security and Its Applications 9.10 (2015): 353-360.

[15]. Nadeem, Aamer, and M. Younus Javed. "A performance comparison of data encryption algorithms." Information and communication technologies, 2005. ICICT 2005. First international conference on. IEEE, 2005.

[16]. Varsha, B. Sri, and P. S. Suryateja. "Using Advanced Encryption Standard for Secure and Scalable Sharing of personal Health Records in Cloud." International Journal of Computer Science and Information Technologies (IJCSIT), ISSN (2014): 0975-9646.

[17]. Hassoun, Youssef, and Hiba Othman. "Symmetric Key Cryptography Algorithms Based on Numerical Methods." Proceedings of NumAn 2014 Conference, Crete, Greece. 2014.

[18]. Mahendra, Leonardus Irfan Bayu, Yehezkiel Khakham Santoso, and Guruh Fajar Shidik. "Enhanced AES using MAC address for cloud services." Application for Technology of Information and Communication (iSemantic), 2017 International Seminar on. IEEE, 2017.

[19]. Khanezaei, Nasrin, and Zurina Mohd Hanapi. "A framework based on RSA and AES encryption algorithms for cloud computing services." Systems, Process and Control (ICSPC), 2014 IEEE Conference on. IEEE, 2014.

[20]. Babitha, M. P., and KR Remesh Babu. "Secure cloud storage using AES encryption." Automatic Control and Dynamic Optimization Techniques (ICACDOT), International Conference on. IEEE, 2016.

[21]. Raj, Gaurav, Ram Charan Kesireddi, and Shruti Gupta. "Enhancement of security mechanism for confidential data using AES-128, 192 and 256bit encryption in cloud." Next Generation Computing Technologies (NGCT), 2015 1st International Conference on. IEEE, 2015.

[22]. Wanve, Balu, et al. "Framework for client side AES encryption technique in cloud computing." Advance Computing Conference (IACC), 2015 IEEE International. IEEE, 2015.

[23]. Singh, Harpreet, and Paramvir Singh. "Enhancing AES using Novel Block Key Generation Algorithm and Key Dependent S-boxes." Cyber-Security and Digital Forensics (2016): 30.

[24]. Nadaf, Reshma, and Veena Desai. "Hardware Implementation of Modified AES with Key Dependent Dynamic S-Box." IEEE ICARET (2012): 576-580.

Hitesh Marwaha"Secure Migration of Data in Cloud Using Enhanced AES Algorithm "International Journal of Computational Engineering Research (IJCER), vol. 08, no. 10, 2018, pp 31-37