International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Issue 01 | 2020

The Application of AES Encryption algorithm in cloud-based services

Rahul Marwaha[1], Praveen Kumar Pandey[2]

[1] Student, Department of MCA, Jain University, Karnataka, India
[2] Assistant Professor, Department of MCA, Jain University, Karnataka, India

ABSTRACT

The World is proliferating in the innovation & information technology sector; data is considered as an asset in the modern world. Data is assets, and assets need to be secure. Modern data is store in data centers. The contemporary world accepts to store data in the cloud for access data all across the globe from remotest areas through cloud-based services. To store data and access data from all around the that requires security to prevent data from stolen. AES encryption and decoding are very high made sure about and quickest strategy. User side encryption is a viable way to deal with a giving security to transmitting to information and put away information. AES (Advanced Encryption Standard) encrypts the data so the only legitimate users can access the data by private keys. Different systems are accessible for accomplishing security by utilizing the capacities of cryptographic methods; it underpins advancements for dealing with the information encryption and decoding calculations. Scramble touchy information before setting it in the cloud. AES is the fastest and securest way of encryption/decryption algorithm. In this paper, we have presented a new security system the utilization of asymmetric key cryptography sets of rules and steganography. In this proposed mechanism AES set of rules is utilized to offer square reasonable wellbeing to records. This arrangement of rules key length is 128 bits. In this paper, we discuss the modern ways to use AES in cloud-based services to prevent data assets from getting stolen. Cloud security used than ever before.

Keyword: ***-AES (Advanced Encryption Standard), Encryption, Cloud Service Provider (CSP) and Cloud Security.***

1. INTRODUCTION-

Cloud-based services are an emerging market which provides vital resources like sharing infrastructure, software applications, and business process on a rented basis is the main idea behind cloud computing. Cloud service's most significant advantages are that cab be scalable, which is cheaper rather than using On-Premises servers. Most of the large companies have promoted their cloud computing platforms and infrastructures for users to deploy their web applications on these platforms. Within the cloud computing world, the virtual environment lets users access computing power that exceeds that contained within their physical worlds.[1]

Cloud Service Provider (CSP) maintains the user application and databases in their data center across the world. CSP provides application maintains and related services like monitoring, Cache memory, Firewalls, different types of storage devices options for better performance, and provide support to extend or use cross-platform application services. CSP gives mainly 3 types of services IAAS (Infrastructure -as-services), PAAS (Platform-as-services), and SAAS (Software-as- Services). These services give chances to deploy all the entire application on the cloud with infrastructure as well. Deployment, all the entire application on the cloud, leads to concern about security.

AES (Advanced Encryption Standard) is an asymmetric encryption algorithm that requires a single key to encrypt or decrypt data. AES has multiple size keys that use multiple numbers of rounds according to their key. 128-bit key, 192-bit key, and the 256-bit key have 10,12 and 14 rounds respectively. There are four steps of encryption that running in the loop according to their rounds. AES is six-time faster than DES (Data encryption standard). That makes AES a better choice for security and data encryption. Cloud computing working on a vast amount of pooled

resources by multiple resources to segregate data with the best encryption methods is the ultimate goal for cloud service provider companies.

There are a few security concerns related to distributed cloud computing. The issues are isolated into two classifications. Right off the bat, security gave by cloud suppliers. Besides, security issues looked at by their clients. They put information in the cloud and endow the supplier. That is why data security on cloud computing is needed. Data security becomes a major challenge in cloud computing to reduce risk. These risks are generally associated with open, shared upload, and distributed environments [2].

2. CLOUD COMPUTING -

Distributed Cloud computing could be quite registering that depends on sharing process assets as hostile having near servers or individual gadgets to handle applications. In distributed Cloud computing, the word cloud is used as a similitude for "the web," that the expression distributed computing signifies "a variety of Internet-based computation," wherever numerous administrations -, for instance, servers, and applications - square measure sent to an association's PCs and gadgets through the web. The design graph for cloud computing has appeared in following Figure 1.

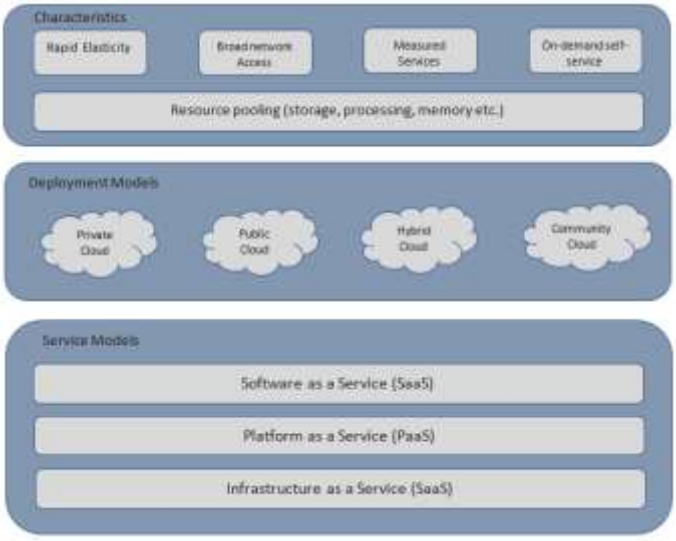

Fig -1: Overview of Cloud Computing

2.1 Cloud Computing Service Models -

There are mainly 3 types of cloud computing service-based models used by a user which are described below-

SAAS (Software as a Service) – This type of service used like hosting an application over Cloud. Users access those applications over the internet.

PAAS (Platform as a Service) – PaaS used by developers to create, test, and deploy Applications overcloud. Developers monitor the traffic usage of applications on each factor which helps to optimize the application over a period of time.

IAAS (Infrastructure as a Service) – IaaS provides users to create their virtual infrastructure overcloud. IaaS gives authority to create customize infra according to their business needs and own security concerns. IaaS used as a private cloud for the organization for specific users and customers.

2.2 Cloud Computing Deployment Models -

There are mainly 3 types of cloud computing deployment-based models used by the user which are described below-
[4]

Private Cloud – Private cloud only allows the inside user or organization to access the cloud service created by an organization for its users and clients. This type of cloud is a custom cloud for their business needs and security concerns.

Public Cloud – Public cloud allows all the users to use the services of the cloud who have Credentials to the cloud. The public cloud has less security and more access to users.

Hybrid Cloud – Hybrid cloud is a combination or mixture of both public and private clouds for different types of activities. For example, financial activities are performed by private cloud and non-essential activities done by the public cloud for more access to the general public. Organizations required both activities are used in a hybrid cloud.

Community Cloud – In a community cloud is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed, and secured commonly by all the participating organizations or a third-party managed service provider [3].

3. RELATED WORK –

Most of the cloud computing services want the excessive performance to place away facts inside the cloud. Storage security refers to protection records on garage media, which is quick to recover. The security of records has to be taken into consideration on software engineers inside the design phase of the cloud service. Not handiest pay interest to facts redundancy or isolation however consider records security. Redundancy is a fundamental measure to secure information protection. Then, Isolation is because specific user information is stored on the same platform, to ensure inter-statistics independency. Data security is likewise critical trouble in Amazon Simple Storage Service.

There are many studies and researches performed to enhance the security of the cloud computing garage and the environment using encryption techniques and other methods. However, there was a moderate improvement in the results of those works evaluating the rapid boom of cloud computing communications. Typically, security fashions in cloud-based totally environments are divided into authentication fashions, facts safety fashions, and access management fashions. Currently, many cloud storage services are realized through outsourcing, cloud storage service operators do not need to build their file storage system, they can use the interfaces provided by the platform to outsource the data store tasks. Some of these platforms are focus on cloud storage, some have much business and cloud storage is a part of them.[4]

Cloud computing environments are likely to suffer from several known vulnerabilities, enabling attackers to either obtain computing services for free (attack against cloud providers), steal information from cloud users (attack against cloud customers data) [5]. Privacy and safety of statistics have usually been a question and cloud computing aren't any exception to this. We consider that the safety and privations of user records ought to be defined by way of the broker. We provide architecture and pointers to boom safety as well as the privations of the owner's statistics.

Once the file is distributed then information is additionally lily-white into several servers. Therefore, here the necessity of data security arises. Each block of the file contains its hash code, victimization hash code will which is ready to} enhance user authentication process; a solely approved person can access the data. Here, the data is encrypted victimization advanced cryptography customary, therefore information is successfully and firmly stick with its cloud. The third-party auditor is used for public auditing. This paper discusses the handling of some security problems like quick error localization, information integrity, information security.

4. RESEARCH OF AES ALGORITHM

Advanced Encryption Standard (AES) algorithm not just for security but also for excellent speed. AES is the current standard for secret key encryption. AES may be a symmetric-key algorithm. it's having various chippers with different keys and therefore the block size. during this plaintext is encrypted with the assistance of AES then the ciphertext which we've got will again encrypt likewise there'll be various round just like the AES algorithm includes 10, 12, and 14 rounds with 128, 192, and 256 key bits. As there are various rounds during this algorithm the plaintext is encrypted over and over and this helps the information to possess the protection [6].

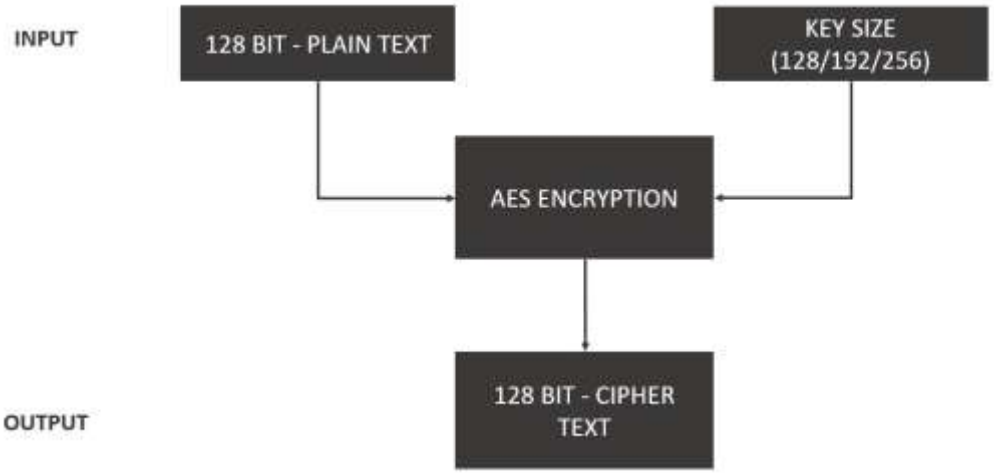

Fig -2: AES Basic Input and Output Structure

AES is one of the foremost economical bilaterally symmetric rules. the benefits It provides sturdy security from attackers. Disadvantages or a significant disadvantage is that its cloud not face up to the attacks like Brute Force, Linear sepulture Analysis as a result of its style wasn't fictitious. There are two main parts of AES Algorithm to understand.

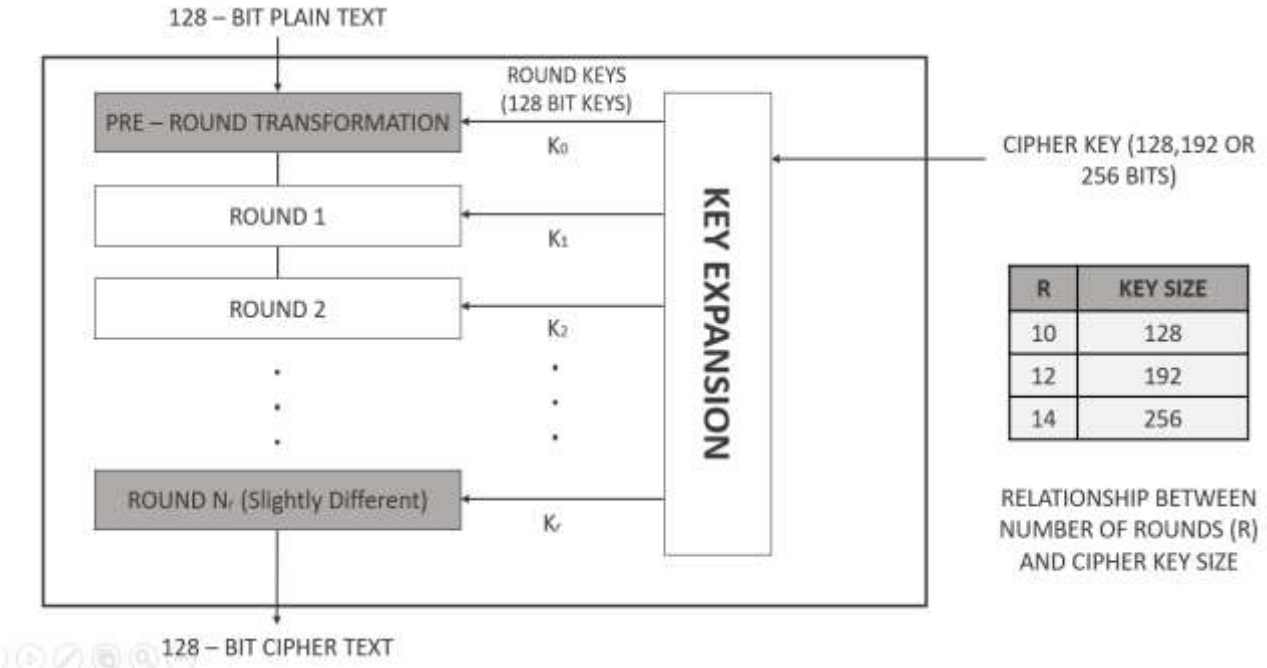

Fig -3: AES Encryption

4.1 Key Generation - The first step of the key generation to convert the data into Hexadecimal because AES works on Hexadecimal. Figure 4 describes how the conversion occurs in AES and making a key state of AES.

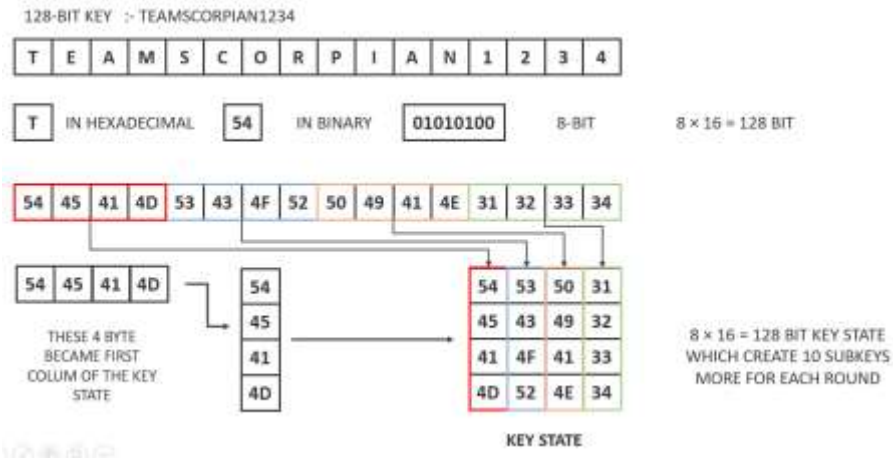

Fig -4: Hexadecimal Conversion of AES

Now the subkeys generation part occurs which divides this key into the next 10 subkeys which used in each of the AES rounds which makes a total of 11 keys for 128-bit encryption. Next step to do rot word which describes in Figure 5 down below.

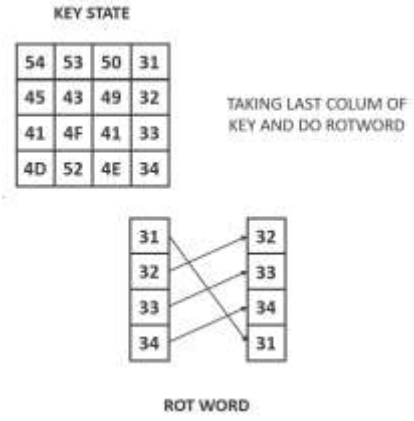

Fig -5: Rot Word

After that rot word takes the column and changes the column with a sub byte table. Take the first character of hexadecimal as a row from the sub byte table and the second character of hexadecimal as a column from the sub byte table and replace it. The Sub byte table is given below in figure 6.

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
10	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
20	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
30	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
40	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
50	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
60	D0	EF	AA	FB	43	4D	33	85	45	F9	02	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	06	24	5C	C2	D3	AC	62	91	95	E4	79
B0	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C0	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D0	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E0	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F0	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig -6: Sub byte (Substitution Table) Table

Now take the First column of Key State and the last Column after sub byte and take the RCON table first column and XOR all their column which make the first column subkey 1. Subkey 0 is the actual key after conversion in hexadecimal. Now take the first column subkey 1 and second column subkey 0 and XOR it which becomes the second column of subkey 1 and so on. Figure 7 shows the sequence of columns.

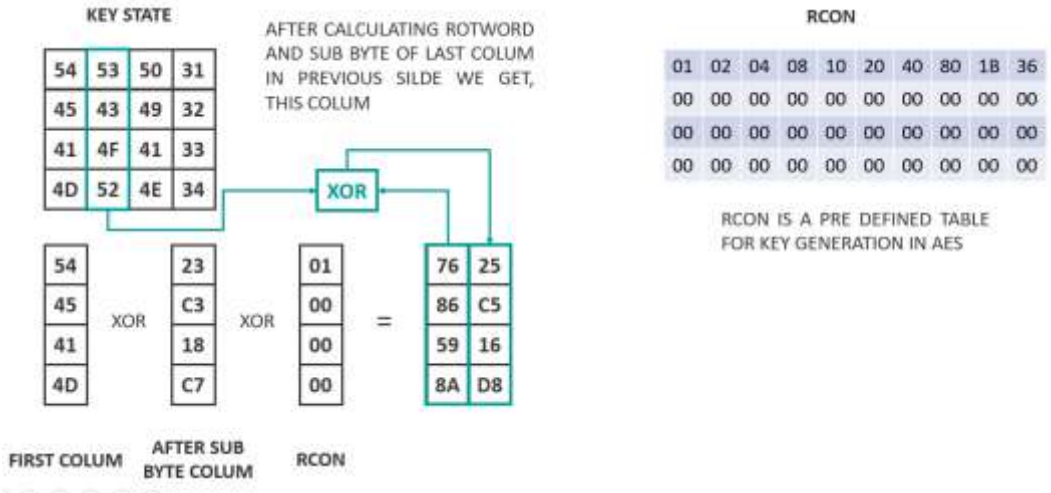

Fig -7: Key State Creation Sequence

Subkey 1 column 1 XOR Subkey 0 column 2 =subkey 1 column 2
Subkey 1 column 2 XOR Subkey 0 column 3 =subkey 1 column 3
Subkey 1 column 3 XOR Subkey 0 column 4 =subkey 1 column 4

Sub key 1 fully created which you can see in Figure 8 below.

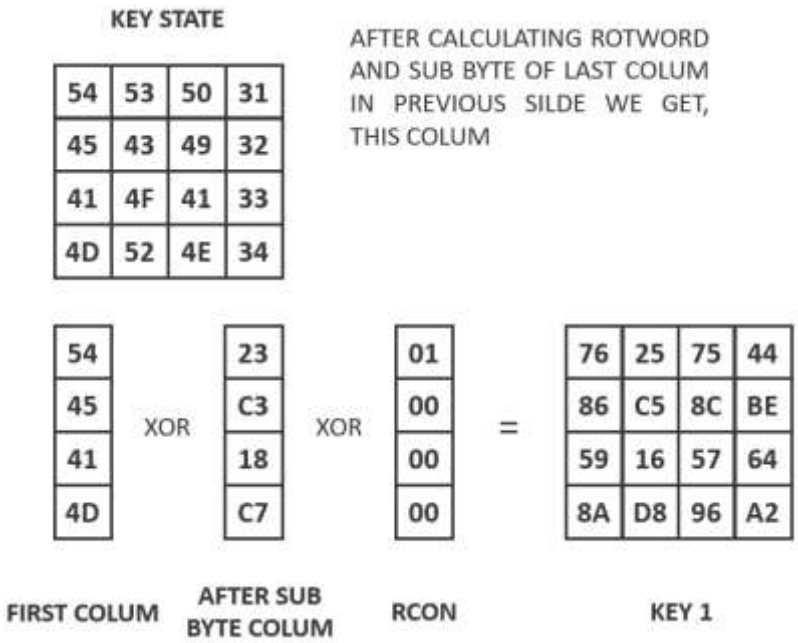

Fig -8: Sub key 1

So now the subkey creates subkey 2 with the same process using the second column of RCON. Subkey creates subkey 3 and so on.

4.2 Encryption Rounds - There are mainly 3 types of rounds in Encryption process.

Initial Round – Initial round only XOR with key 0 and 128-bit block message hexadecimal state only no other steps are involved which you see in Figure 9 below.

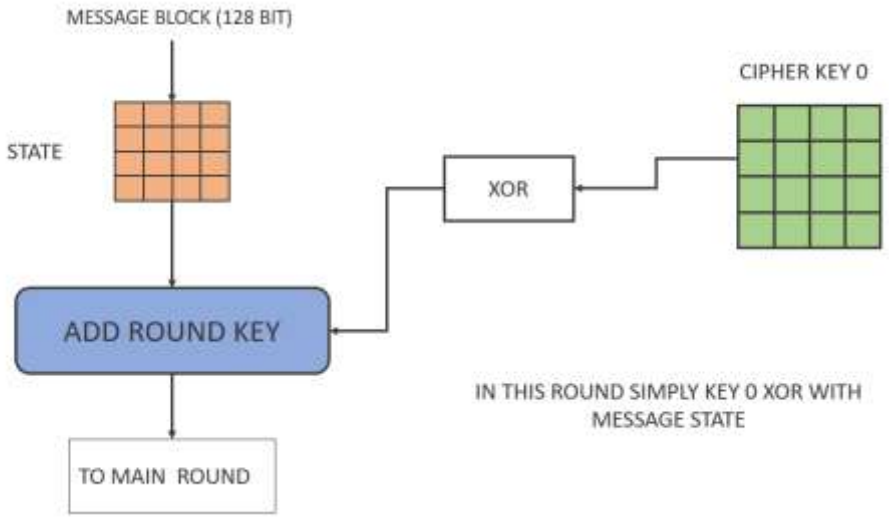

Fig -9: Sub key 1

Main Rounds – Main round Include Sub Bytes, Shift Rows, Mix Columns, and Add Round Key which repeats its self it depends on the key size how many times loop execute. In below Figure 10. Main rounds you can see the sequencing process.

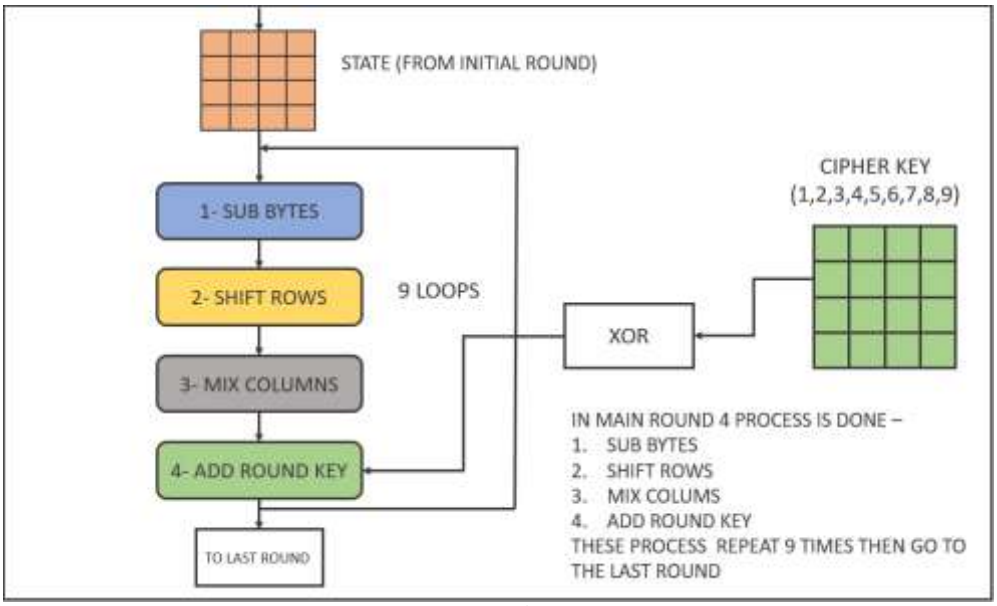

Fig -10: Main rounds of AES Encryption

Last Round – Last round Include Sub Bytes, Shift Rows, and Add Round Key. The last round does not include the mix column. In below Figure 11. Main rounds you can see the sequencing process.

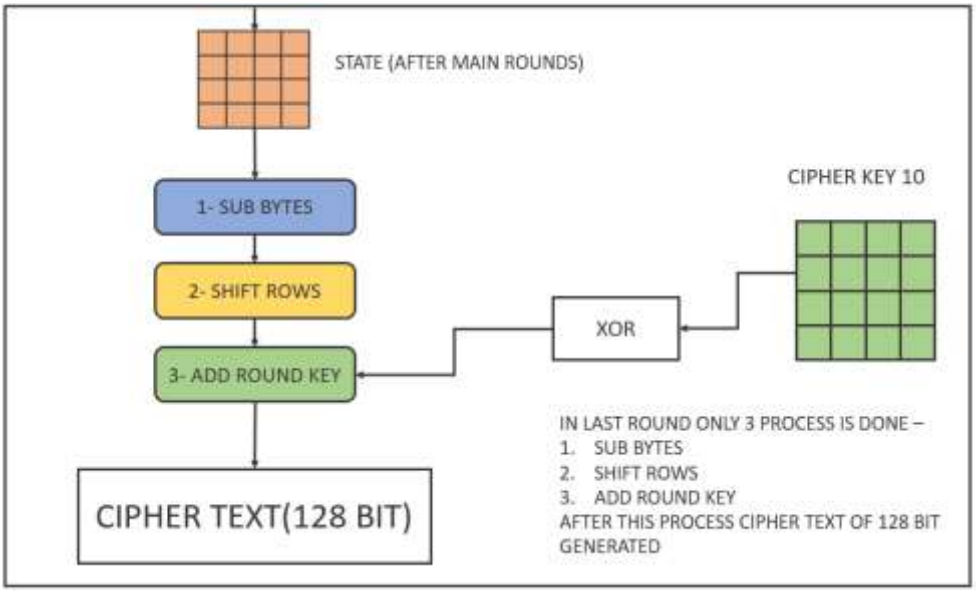

Fig -11: Last round of AES Encryption

4.3 Encryption Steps - There are mainly 4 steps used in main round of Encryption process.

SubBytes – A non-linear substitution step where each byte is replaced with another according to a lookup table (S-box) [1]. Sub bytes change each element of the table of the Substitution table. Taking the first character of hexadecimal as row and second element as a column from message after converting into hexadecimal 4*4 Matrix. In the below Figure 12, you can see how the Substitution box works.

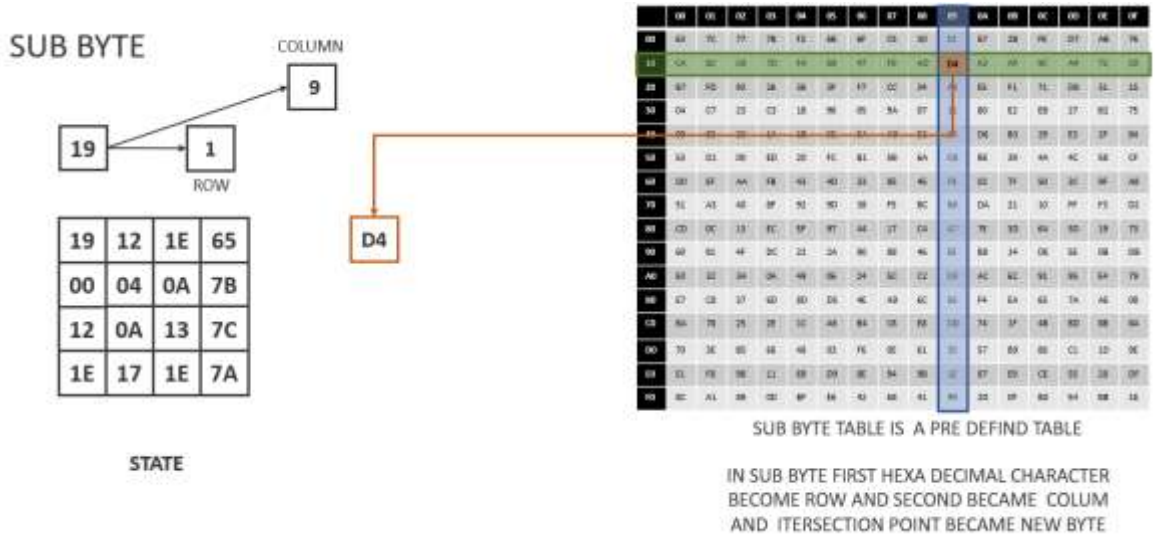

Fig -12: Substitution Box or Sub bytes Process

AddRoundKey – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule. Cipher Key is created by Key expansion method. That is the result of Sub keys to perform this Step Each element is XOR with Cipher key in below Figure 13 you can see how the AddRoundkey is performed.

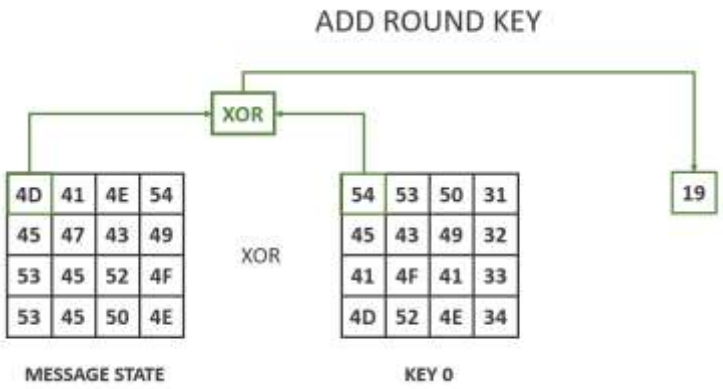

Fig -13: AddRoundKey Process

ShiftRows – A transposition step where each row of the state is shifted cyclically a certain number of times [1]. Here each row is shifted to the left in increasing order. The left out taking the place of moving elements in below Figure 14 you can see the process.

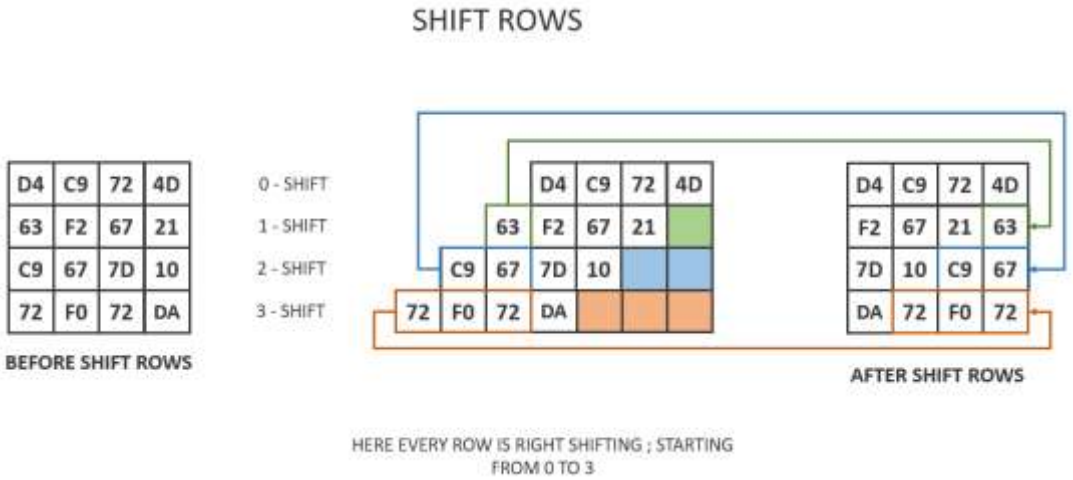

Fig -14: Shift Rows Process

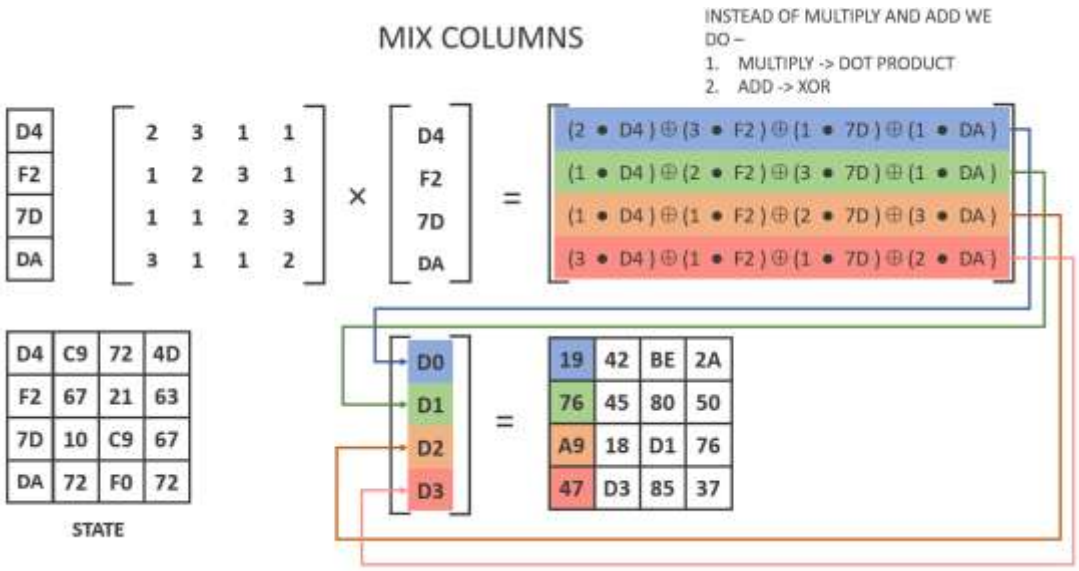

Fig -15: MixColumns Process

MixColumns – A mixing operation that operates on the columns of the state, combining the four bytes in each column [1]. Here message state is multiplying by another matrix, there XOR takes place of plus in matrix multiplication and multiply takes the place of Dot Product. If the Dot product is bigger than 8 bits product is reduced by reducing polynomial (X^8+ X^4+ X^3+ X^1+ X^0). In below Figure 15. You can see how this can be done. In each dot, product number is greater than 1 is subtitled by their respective table. Elements dot product with 1 gives the same result.

5. CONCLUSION –

In this paper, we've offered that the tied down data system to disentangle the matter of data security and protection in distributed computing. With this paper, users will offer higher security to data than the existed framework. to flexibly protection and security to transmittal data additionally as data keep on cloud. we've depicted customer feature cryptography and decipherment strategy abuse single mystery key. A short time later, during this paper, we tend to investigate AES cryptography and decipherment topic to make cloud clients data made sure about and conjointly ensure the data security inside the cloud. Modern information is store on server farms. The contemporary world acknowledges storing information in the cloud to get to inform the whole way across the globe from remotest regions through cloud-based administrations. To store information and access information from all around the that expects security to keep information from taken. AES (Advanced Encryption Standard) scrambles the information so the main genuine clients can get to the information by private keys.

6. REFERENCES –

[1]. Abha Sachdev, and Mohit Bhansali. "Enhancing Cloud Computing Security using AES Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.

[2]. L. Kacha and Abdelhafi Zitouni, "An Overview on Data Security in Cloud Computing," Cybern. Approaches Intell. Syst., vol. 661, pp. 250–261, 2017.

[3]. Mr. B. Thiyagarajan, Mr. Kamalakannan.R. "Data Integrity and Security in Cloud Environment Using AES Algorithm" ICICES2014 - S.A. Engineering College, Chennai, Tamil Nadu, India.

[4]. Zhiyi Fang, Yao Sun, Yujing Sun, Jianming Yang. "The Research of AES algorithm and application in cloud storage system" 2nd International Conference on Science and Social Research (ICSSR 2013).

[5]. Praveen Ram and Sreenivaasan, Department of Computer Science Engineering Rajalakshmi Engineering College, Anna University Chennai, India, ―Security as a Service (SasS)‖ 2011 IEEE.

[6]. A. Singh, P. Gupta, R. Lonare, RahulKrSharma, and N. A. Ghodichor, "Data Security in Cloud Computing," Int. J. Emerg. Trends Eng. Manag. Res., vol. 3, no. 2, pp. 1–5, 2017.