Security analysis of cloud computing based on rk-aes algorithm.

18MIS1001-Jahnavi Sri Kavya , 18MIS1033-Swathi J , and 18MIS1105- Dutta Yasaswi

Vellore Institute of Technology, Chennai
*swathijayaprakash2000@gmail.com
*yasaswidutta666@gmail.com
*jsk.bollimunta@gmail.com

ABSTRACT

A cloud platform has various threats and vulnerability. In the cloud platform multiple users are given storage at a single server, so we really don't know with which kind of user we are sharing the server. There are chances that we might share the server with a malicious user. So, to overcome this we are using encryption and decryption of files before uploading inside the cloud. As AES is one of the common encryption techniques, there are also many attacks done on advanced encryption technique that's the reason why we have come up with an idea of Symmetric Random key Generator (SRKG), which actually generates a random key every time we encrypt and decrypt the file, so basically using the random key generation in advanced encryption standard algorithm is known as RK-AES. We have also compared the RK-AES with AES and justified how can this RK-AES overcome the vulnerabilities of the files uploaded in cloud platform and a partial implementation of encrypting and decryption of the file is also done.

Keywords: GCM- Galois/Counter Mode, Rk-AES- Random key advanced encryption standard, ECB- Electronic Code Book, Pt- plain text, Ct- cipher text ,CBC- Cipher Block Chaining.

1. INTRODUCTION

Cloud technology is used in various architectures, services with upcoming technologies. However,there are different kind of concerns on security issues which are related to computed architectures of cloud.the main problem of cloud data storage is security.therefore, the data centres in cloud computing should have an exposure of various mechanisms in cloud environment
Cryptography, which is major sector in the field of security. It has a services such as confidentiality, authentication and soon on. There are two majorly divided components named them as cryptography and cryptanalysis. As we can seeing the strength of technology in today's world, there is much needed security all of such instances happening ,in turned there is a need of building new cryptography algorithms and cryptanalysis as well to measure and track the progress of built cryptographic algorithms. All this together is in the form of cycle that exhibits cryptography and cryptography analysis. All the information of technology applications helps for security of cryptography algorithms by converging. And the cryptographic is again divided into two majorly components named them as

1. Block ciphers and stream ciphers based structure of the message

2. Symmetric and asymmetric based on number of keys required for the algorithms.

While we build up any of cryptographic algorithm, there must be concern on size of the key, message and the number of rounds that we perform on particular application. We mostly concentrate on the size key that we select in the cryptography algorithms. It's because , there are instances where you select a weak key , there are quite few chances of revealing the plain text to third party users in minimum amount of time hence information gets leaked. It is known that cryptography has support of brute force in any of attacks. But, the complexity it is going to possess is much higher when compared to other application in cryptanalysis. There is no point of encouraging the weak keys in cryptographic algorithm that we perform. Since, the attacker's job is to track the plain text either by knowing cipher text or breaking the key. There are future instances that may encounter like, the algorithm selects the strong key which gets weakens by third party users by applying some computation tactics. The cryptographic algorithm stay in such a way that things mentioned should be avoided and shouldn't let it happen in of case.
Basically, the algorithms of cryptography has an impact on its structure and its functions. It's also uses the Boolean functions in algorithms when it comes symmetric property, rather than focusing only on AND, OR, NOT and XOR these gates. Its helps in creating the generic functions of algorithm initially. Though, the selected key is stronger, there is still a chance of plain text getting hacked. The cryptographic algorithm generators get to add new features in order to give much strength to ciphers. One of such solution to any of those problems is Physical Unclonable Functions for given requirements on cryptanalysis. In order to provide strength to ciphers, there are few characteristics such as nonlinearity, correlation and propagation. Physical Unclonable functions are useful for Field Programmable Gate Arrays (FPGA) implementation as it is more related to hardware. Not that really applicable to cryptographic algorithms. There is similarity in cryptographic approach and the PUF. Here, what makes PUF inactive is that the way is taken forward and its explanation are diverse. But then, it can be used in randomness of the key in encryption and decryption of cryptographic algorithm that makes it acceptable though.
In this paper, in order to get the randomness of the key generation we have followed the Advanced Encryption Standard. This has followed by the Symmetric Random function generator (SRFG).

1. Practicing of random key generation in AES Algorithm.

2. Making sure of propagation, immunity and high non-linearity.

2. FEATURES OF RK-AES ALGORITHM

1. In the RK-AES algorithm, plain text is represented in the form of blocks and gets processed one by one.

2. the size of the block size = 128 bits of plain text. it also allows 192 and 256 bits.

3. RK-AES is also uses a key in each and every round of plain text in order to get cipher text.

4. Number of rounds in RK-AES is 10 rounds, 12 rounds for 192 bits and 14 rounds for 256 bit keys.Other than last round in the each case, rest all stay the same.

5. the size of the key =128 bits/16 bytes/4 words and the key is processed in the form of words and the size of each word is 32 bit.

6. Number of sub-keys used are 44 sub-keys and each of the sub-key possess 32 bits/1 word/ 4 bytes of size

7. We use 4 sub-keys in each round.before that , we use pre-round calculation which is 4 sub-keys and eventually , we get a cipher text of 128 bits.

8. Each round of processing consists of a single byte S-boxes step,a row -wise shifting permutation step, a column- wise mixing step and adding the random key generated at the end.

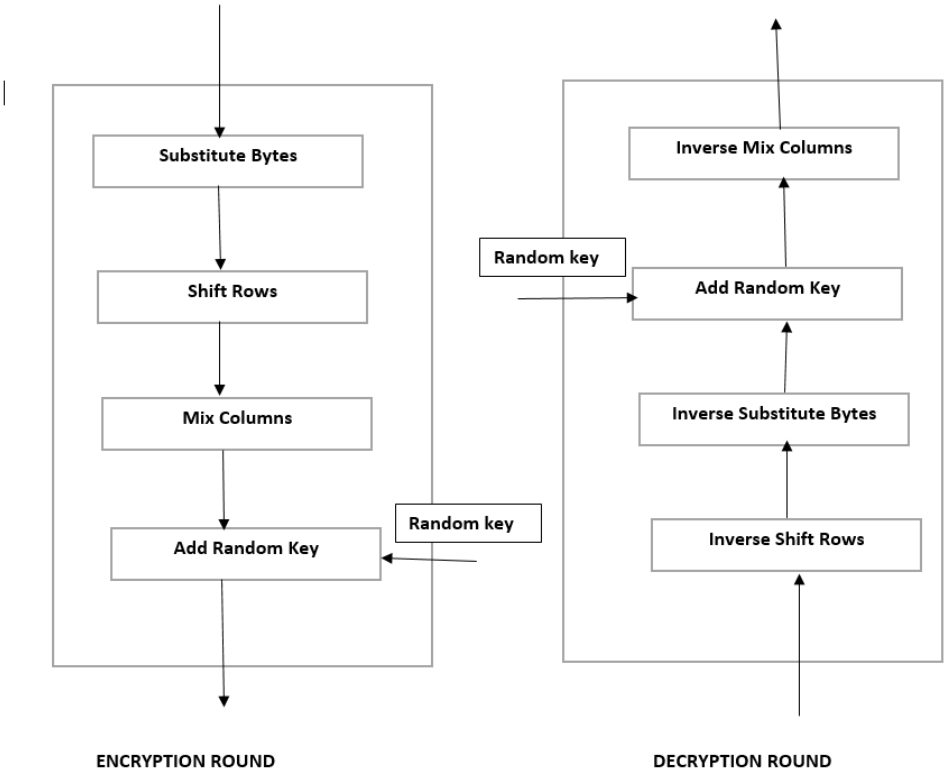

FIGURE 1. General Block Diagram of RK-AES

The plain text which is of 128 bit prepares for XOR operation with 128 bit random key generated which is also 128 bit. To the Obtained ,we have to apply substitute keys(S-Boxes).it has a size of 128 bit of input and output as well. And then we apply circular right shifts based on default shifting of rows.then goes with mix columns where you get to multiple with default matrix(4*4). consider a single word from output obtained from s-boxes and perform multiplication.finally, we are suppose next generated random key to the output obtained from Mix columns. This whole set of operation is said to be single round function in RK-AES. this has to repeated 9 more

times to complete the task.
Whereas, in the tenth round , we vomit the mix columns operation.We directly add the random key generated to the shift rows
128 bit of plain text is stored as input arrays which is represented in 4 cross 4, rows and columns.this is how we represent plain text where each block is 1 byte=16 bytes/128 bits

inp-0	inp-4	inp-8	inp-12
inp-1	inp-5	inp-9	inp-13
inp-2	inp-6	inp-10	inp-14
inp-3	inp-7	inp-11	inp-15

Intermediate results are stored in state array which are basically called substitutes boxes(S-boxes).

Sub-0,0	Sub-0,1	Sub-0,2	Sub-0,3
Sub-1,0	Sub-1,1	Sub-1,2	Sub-1,3
Sub-2,0	Sub-2,1	Sub-2,2	Sub-2,3
Sub-3,0	Sub-3,1	Sub-3,2	Sub-3,3

1. S-0,0 is zeroth bit of zeroth word
2. S-1,0 is first bit of zeroth word
3. S-2,0 is second bit of zeroth word
4. S-3,0 is third bit of zeroth word
5. S-0,1 is zeroth bit of first word
6. S-1,1 is first bit of first word
7. S-2,1 is second bit of first word
8. S-3,1 is third bit of first word
9. S-0,2 is zeroth bit of second word
10. S-1,2 is first bit of second word
11. S-2,1 is second bit of first word
12. S-3,1 is third bit of first word
13. S-0,2 is zeroth bit of second word
14. S-1,2 is first bit of second word
15. S-2,2 is second bit of second word
16. S-3,2 is third bit of second word
17. S-0,3 is zeroth bit of third word

18. S-1,3 is first bit of third word
19. S-2,3 is second bit of third word
20. S-3,3 is third bit of third word

The state array with four rows and columns of 16 bytes /128 bits The input of s-boxes is 8 bits.and the first four bits is considered as row number and next four bits is said as column number. The output of s-boxes is turned out to be 8 bits. Similarly, The output arrays represented as

output-0	output-4	output-8	output-12
output-1	output-5	output-9	output-13
output-2	output-6	output-10	output-14
output-3	output-7	output-11	output-15

The random key is of 128 bits or 4 words.consider ,the key also arranged in the form of an array of 4 cross 4 bytes.just like input block,the first word from the key fills the first column followed by other columns and so on. there is an expansion of four column word of the key array to 44 words
the first ten rounds uses 40 words and the rest 4 words is used by pre-round key generation.

K-0	K-4	K-8	K-12
K-1	K-5	K-9	K-13
K-2	K-6	K-10	K-14
K-3	K-7	K-11	K-15

1. The first four bytes from the encyption key consists the word W0, the next four bytes is consider as W1 and so on.
2. this algorithm gradually expands the words[w0,w1,w2,w3] into 44-word key schedule.
3. With these given words[w0.w1.w2.w3] of bit wise gets XOR with the input array block before the round-based random key generation begins.
4. The rest of 40 words present in the Key schedule can make four words at a time in each of the 10 rounds.
5. the same thing happens for decryption as well , except the fact that it has reverse the particular we have been follwing so far in the given key schedule.

W-0	W-1	W-2	W3	W4	——	W-42	W-43

In the shift rows, performing of circular right shift depends on the row.For an instance,first row gets shifted for about and then second row about of 2 bits and so on like wise.

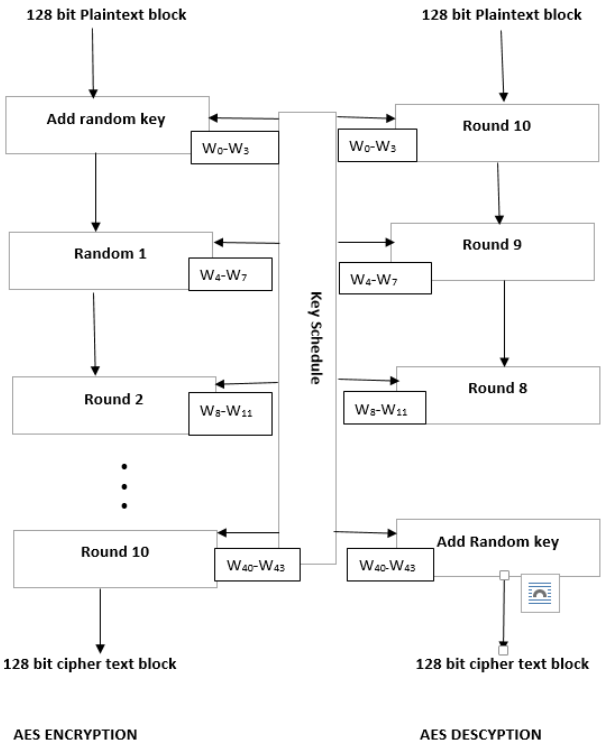

FIGURE 2. Random key generation

Sub-0,0	Sub-0,1	Sub-0,2	Sub-0,3
Sub-1,0	Sub-1,1	Sub-1,2	Sub-1,3
Sub-2,0	Sub-2,1	Sub-2,2	Sub-2,3
Sub-3,0	Sub-3,1	Sub-3,2	Sub-3,3

Sub-0,0	Sub-0,1	Sub-0,2	Sub-0,3
Sub-1,1	Sub-1,2	Sub-1,3	Sub-1,0
Sub-2,2	Sub-2,3	Sub-2,0	Sub-2,1
Sub-3,3	Sub-3,0	Sub-3,1	Sub-3,2

The output obtained from the circular right shift will be input for mix columns.Just take one word from the above input .Apply default multiplication.The below matrix is multiplied with one word obtained from circular right shift.and we do this for all four words. which in turns returns a four cross four static array.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

The obtained static key gets on XOR operation with the next round random key that is generated. Get the first column of state array ,perform XOR operation with first column of key which us new resultant array. and perform same block diagram as we

discussed above.

2.1 BLOCK DIAGRAM

After inputting the files from local computer, we are encrypting the files. By encrypting we mean we are using RK-AES algorithm using GCM mode. If the file is encrypted, the file is uploaded in the cloud server. And the random key is generated before every encryption process. If the key is valid, then the file is decrypted or else its not decrypted.

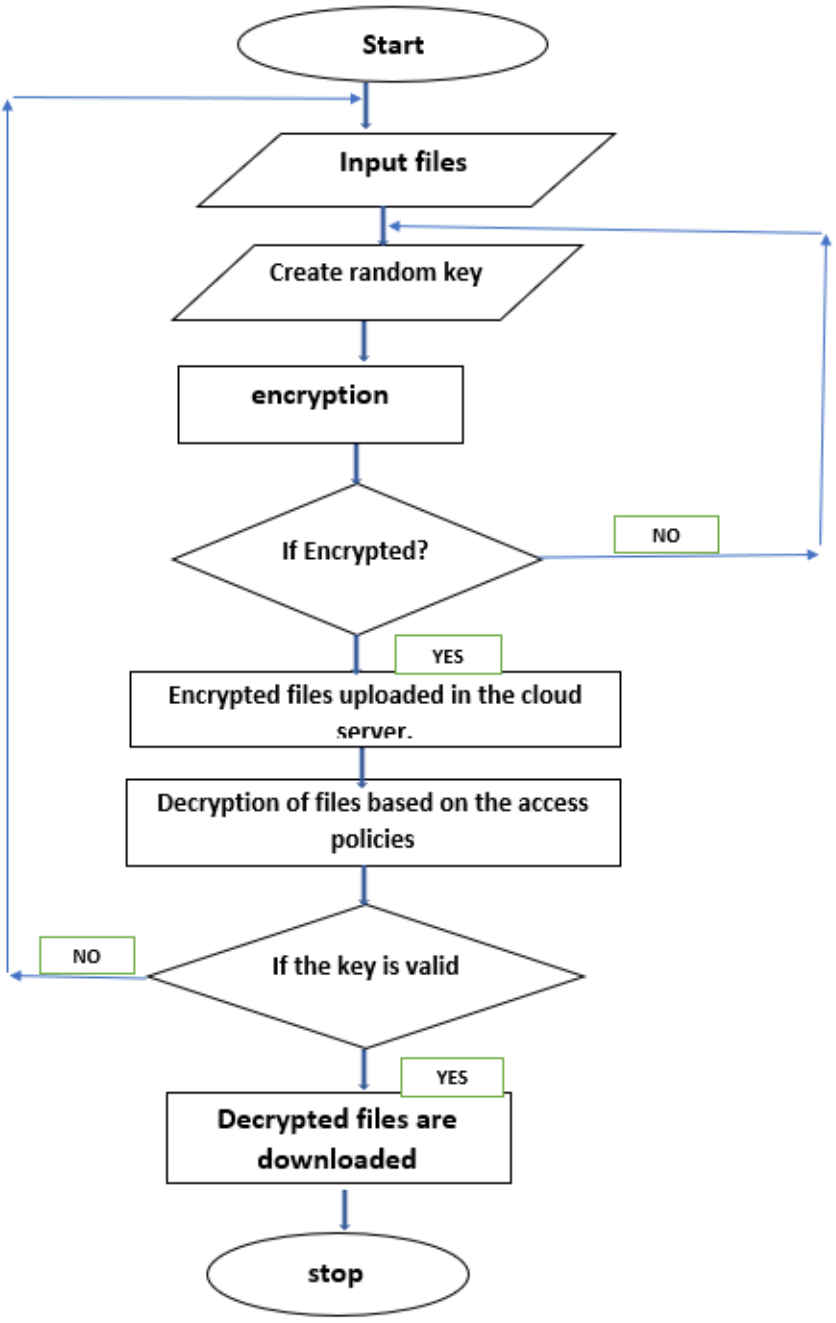

FIGURE 3. Flowchart

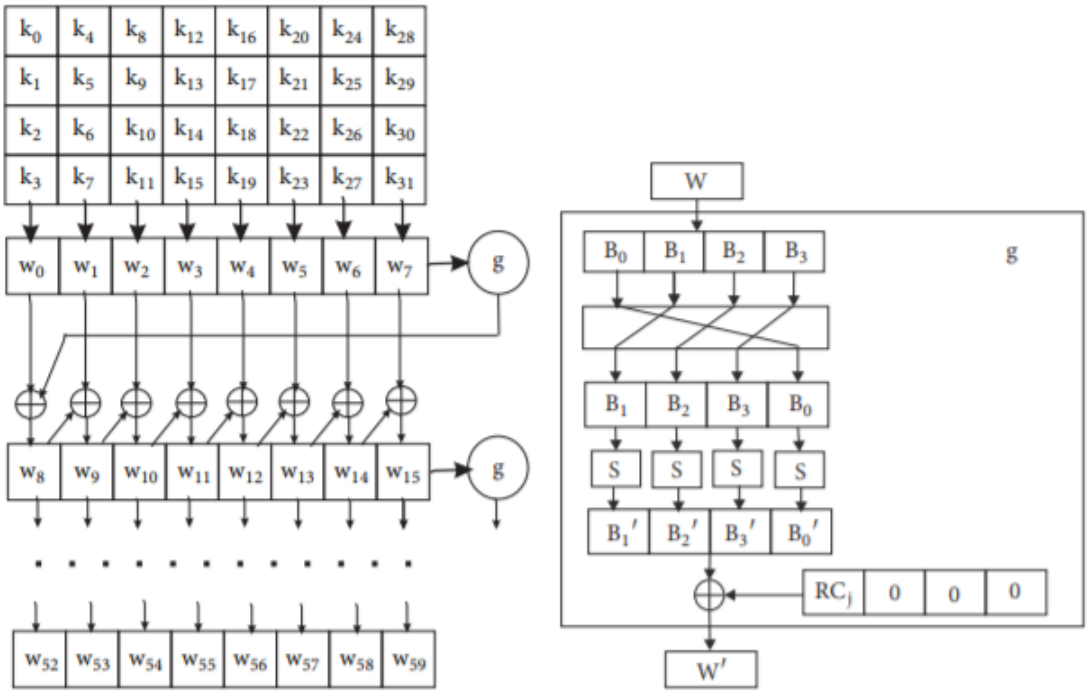

FIGURE 4. Key Expansion For 14 Round AES

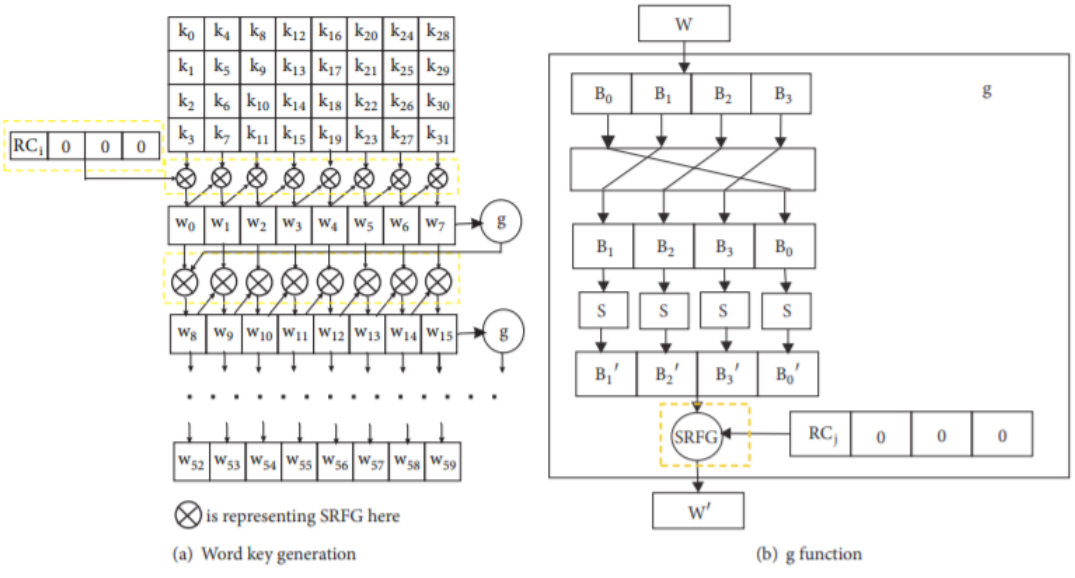

FIGURE 5. Key Expansion For 14 Round RK-AES

3. HOW RK-AES HELPS PROTECTING DATA IN CLOUD

Numerous company and customers will store their particular and most important information's on cloud and these stored data's are also approached by many users, hence its very difficult to store the data safely in the cloud. so, in that case to enhance security to the cloud platforms many encryption and decryption algorithms are available and one of the common one among them are AES. there are many possible attacks

available on the current advanced encryption standard. in order to protect the users data in much secure way possible,we are using random key generator in advanced encryption standard using GCM mode. so, every time a a user opens or uploads the file in the cloud the encryption and decryption is done and a new key is generated every time the file is encrypted or decrypted. so, we'll detailly see the security analysis of cloud and RE-AES under this topic.

3.1 SECURITY ANALYSIS IN CLOUD

If we wish to grow the security in the cloud related areas, we should 1st be clear with in which areas of cloud we are using the security and how it works. So, the main goal of security in cloud is integrity, confidentiality and availability.

Integrity: integrity is basically a degree of trust that the user has in cloud and its data. And is protected against any kind of unconscious or conscious changes without authorization. This process should actually be well-designed distributed system, a good audited code and a strong access control mechanism.

Confidentiality: confidentiality meaning keeping the data private. This is reinforced by technical tools like access control and encryption.

Availability: availability is a mode of being able to utilize the set-up as expected. this is supported by capacity construction and robust architecture.

Accountability: this is the responsibility that should be taken by any individual. It is supported by strong identity, access control and authorization and also with the ability to log the transaction and audit their own logs.

Assurance: assurance refers to the need the system acts as anticipated. This is trusted by the careful process mapping from technical to legal agreement and by computing architecture in the cloud.

Resilience: resilience is basically a system that allows us to manage with the security threats. This is basically supported by the diversification, real-time forensic capacity and redundancy.

3.2 SECURITY ANALYSIS OF RK-AES

As we are using the RK-AES with the GCM mode, this encryption standard is considered much safer than the AES. The GCM mode also holds up further authenticated figures. this mode is also called as AEAD by Cryptographers. The output of an AEAD and the fucntion refers to authentication and cipher text as well to be mentioned as tags, which is much important (along with the key and nonce, and optional additional data) to decrypt the plaintext. the security analysis on the modified AES key expansion.Here we are considering two attacks:

1.attack analysis due to Related key-
the Related key attacks actually uses the differential relations or linear relations in the

keys to find the original key.
Let nz be a known nonzero word difference for input and o be an output difference of S-box for the input difference nz. while running the attack with this kind of dissimilarity, the difference of o could possibly be one of 2 to the power of (14) 1 values, due to the symmetry of the XOR operation is used in the general AES-256 algorithm, the difference in nz could possibly be one of 2 to the power of(15) 1 dissimilarities , which includes the whitening of keys. If such dissimilarities are present in the bounded value zone, then the probability of the key is also gets increased. but,in our modifies advanced encryption standard algorithm, the feature of non-linearity will increase this dissimilarity and hence, searching the key space also gets drastically increased. for a 32 bit word, the complexity of searching in key space increases and the formula is given as follows:

Complexity For Key Space Search= 2power(32).2power(Nl)

where Nl is the value of non-linearity in the proposed AES key expansion and the average value of Nl = 20.7. hence, the complexity turns out to be 252.7, which is technically higher than the differential attacks key searching complexities on advanced encryption standard. so, This proves that the algorithm that we proposed is protective in differential attacks.

2.Fault analysis attacks-
here in fault analysis attack part, we are only concentrating on the fault injection part present on the key bytes. so, here we are assuming for a random original key byte, one of the fault key byte is been injected on the key matrix. And the fault in the input is been taken from the input where in all or either one bits byte or zero bits byte. When it comes to original Advanced Encryption Standard Algorithm, if we use fault and biased inputs it just shows the relationship between the word byte and the even words of round. since, in an original Advanced Encryption Standard, the space in key recovery is decreased with less complexity as per the literature review we have presented.

4. PROS AND CONS

Pros:

• Extremely secure- we are using a random key advance standard encryption, which is extremely secure.
• Difficult to find the key- as we are using the random key, a new key is generated every time a user is encrypting and decrypting. So, it's very difficult for the 3rd part or malicious attacker in the cloud to find the key.
• If we use 128 bit, then for decrypting the content the attacker should try 2 to the power of 128 attempts needed to break it.
• cloud needs a reliable internet: To use our cloud services, we first need a good internet connection which has a good bandwidth for downloading/uploading files from the cloud service.
• Relatively fast- encrypting and decrypting the symmetric is actually easy to do and

gives us a good reading and writing performance.
• Reliability- Reliability reflects with user's infrastructure present in the cloud and availability of applications and services. the reason behind cloud providing numerous services is due to its redundant infrastructure.
• Minimum management and low budget: as we are using cloud platform, people do not need to invest on the infrastructure, which means the cost we spend to manage them also gets reduced gradually. According to any infrastructure which adapts cloud must also recruit one qualified staff who can deal with these cloud issues. Always when it comes to cloud, the infrastructure is only responsible for its cloud uses.

Cons:

• If in case, a person gets to encrypt and find the symmetric key, then in this case it might cause a very big problem, the malicious person will possibly decrypt the content of our files and can easily access it.
• Security: securing our data's from the attackers is always a night mare to everyone . As cloud services are made out to be public. then it totally depends on the provider and the way he handles the data. • choosing a right cloud service for our business is very necessary. And that should be done before finding a provider who accepts its compliance and security data policies.
• finite control on infrastructure: as we don't own the infrastructure of cloud, we'll be provided with only limited control. according to the access control policy we'll be assigned a role.
• limited flexibility: even though the cloud platforms gives a large amount of services to its user. but, when the user consumes it, it shoots up with lot of restrictions.

5. RELATED WORK

A well-known cryptographic algorithms that has been widely used is AES. This has an ability of providing security to web applications. Though, it has been used widely all over, there are attacks noted under AES algorithm.
The attacks have been recorded under masked algorithm of it used by zero values sensitivity model. The proposed structure or model of AES algorithm which is masked has an ability of breaking of S-boxes part of key generation. This obtains because of merging of sensitivity approach analysis and zero values sensitivity approach [8]. It is clearly seen that this has been happened because of zero values sensitivity approached which leads to revealing of particular key.
Well, authors have encountered errors in columns of AES, added that they get misplaced which leads to fault approach [9]. It also been said that this kind of better when compared to other attacks on AES [10-12]. There are few improved versions of AES, shown in [13] papers. Few researchers have found results on fault input generation of random byte in the eighth round which is enough for deducing of block cipher. It is said that the existence of two faulty cipher texts generated, respective key gets revealed without any of brute-force applied. This has explained in paper [14]. There are AES recovered analysis shown in the paper [1]. This paper has driven with complexity of attacks in AES-256(key which has length of 256 bits).In case ,there is an

availability of two random related keys and to get over the complexity of 239, the 9 round version of AES-256 would work fine. 245 time complexity would be work fine for AES-256 version which has 10 rounds. The very much improved version of it has discussed in paper [2]. It is been said that AES gets weak in starting of the round and get minimized to 7th from 9th which is against round transformation and ex
pansion of respective key.
In the paper [3], authors have discussed about pseudorandonmess approach in order to provide much security to algorithms but the problem is generating a biased keys opposed to AES rounds. The key get revealed later on by a computation methods, it's because of biased keys that is capable of deducing the randomness of key. We have seen attacks happened because of faulty based injections, the solution to it have shown in this paper [6]. When the selected criteria is independent on the both s-boxes and inverse s-boxes which leads to 95 percent fault assurance. Recently, authors have analyzed on the solutions of fault injections [25].
After much analysis on how different are all the attacks on AES, it is true that fault injection get reveal the key in more efficient way. Intend, there fault injections seek help from biased input to differentiate the sub keys and other parts of an algorithm. As we know that AES work on with the 8-bit bytes, these can be compiled to some extent. Biased inputs join with fault injection make up a problem while processing it, those get to do with working of differential linear analysis and at the end, the key is revealed. In order to take over all of such problems, there is new feature that is added to AES which is randomness and symmetric property in the output, prominently in keys generation. This improved version is called as RK-AES algorithm. Though, some part of part is known to attackers and practicing a fault based. The obtained fault based gets turned into symmetric property output instead of revealing the actual key or can be plain text.

6. IMPLEMENTATION AND RESULTS

We generated random keys using random key generator and performed the AES algorithm with encryption modes.The comparison was performed of authenticated encryption modes Electronic Code Book (ECB) and Gallios/Counter Mode (GCM) and used GCM mode in implementation because the main goal of security in cloud computing is authenticity,integrity,Confidentiality. AES with GCM provides all these properties and also it is more secure and faster than other modes. We used 128 bit tag length with key size 16 bytes (128 bits) and Initialization vector of size 12 bytes.

6.1 GCM MODE OPERATION:

GCM is said to be in CTR mode generally,it has got to measure the authenticity in a sequential manner while performing the encryption. So, it is a combination of CTR and authentication tag and it does not require padding. This authentication tag size is an important property in security. So, the size of the authentication tag should be at least 128 bits long.

6.2 RESULTS:

Results on implementation are the key will be generated randomly for every run and perform the encryption and decryption of the file uploaded in cloud. We also generate Initialisation Vector randomly so that for every run it gives different cipher text for an identical message.

7. CONCLUSION

Cloud computing is evolving much denser in the field of information technology. When it comes to identifying security challenges is been such a big task in cloud computing with huge amount of services. The paper has a research work on providing to security and privacy to applications by executing RK-AES algorithms to user level. Focusing on intellectual property issues and assuring the trust Of the User. It is required to verify the encryption and decryption of data in RK-AES. Whether the plain text generated is correct or not, do the sender and receiver has communicated or not .RK-AES ensures of transferring the information more securely and accurately. The most vital part of this paper is key expansion and generating randomness to key generation. The practice of SRFG being a function in AES has proved it to be beneficial. This paper eventually shows you that there 53.7 percent of better having confusion property and avalanche effect than actual AES algorithm. It is proved that RK-AES efficient in cryptographic algorithms by generating a random key which is stored in round keys in every round and applied it to decryption respectively, Rather than using symmetric property sharing same key in both encryption and decryption in AES.

REFERENCES

[1] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, "Key recovery attacks of practical complexity on AES256 variants with up to 10 rounds," in Advances in cryptology— EUROCRYPT 2010, vol. 6110 of Lecture Notes in Comput. Sci., pp. 299–318, Springer, Berlin, 2010..

[2] J. Cui, L. Huang, H. Zhong, and W. Yang, "Improved related-key attack on 7-round AES-128/256," in Proceedings of the ICCSE 2010 - 5th International Conference on Computer Science and Education, pp. 462–466, 2010.

[3] S. Sahmoud, "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher," Int. Arab J. e-Technol, vol. 3, pp. 17–26, 2013.

[4] S. Raza, L. Seitz, D. Sitenkov, and G. Selander, "S3K: Scalable security with symmetric keys - DTLS key establishment for the internet of things," IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1270–1280, 2016.

[5] T.W. Cusick and P. Stanica,Cryptographic Boolean functions and applications, Elsevier/Academic Press, 2017.

[6] H. Mestiri, F. Kahri, B. Bouallegue, and M. Machhout, "A high-speed AES design resistant to fault injection attacks," Microprocessors and Microsystems, vol. 41, pp. 47–55, 2016.

[7] J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, “A survey on silicon PUFs and recent advances in ring oscillator PUFs,” Journal of Computer Science and Technology, vol. 29, no. 4, pp. 664–678, 2014.

[8] Q. Wang, A. Wang, L. Wu, and J. Zhang, “A new zero value attack combined fault sensitivity analysis on masked AES,” Microprocessors and Microsystems, vol. 45, pp. 355–362, 2016

[9] G. Piret and J. Quisquater, “A diferential fault attack technique against spn structures, with application to the AES and khazad,” in Cryptographic Hardware and Embedded Systems - CHES 2003, vol. 2779 of Lecture Notes in Computer Science, pp. 77–88, Springer, Berlin, Heidelberg, Germany, 2003

[10] J. Bl¨omer and J. Seifert, “Fault Based Cryptanalysis of the Advanced Encryption Standard (AES),” in Financial Cryptography, vol. 2742 of Lecture Notes in Computer Science, pp. 162–181, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[11] S. Patranabis, A. Chakraborty, D. Mukhopadhyay, and P. P. Chakrabarti, “Fault Space Transformation: A Generic Approach to Counter Diferential Fault Analysis and Diferential Fault Intensity Analysis on AES-Like Block Ciphers,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1092–1102, 2017

[12] C. Giraud, “DFA on AES,” in Proceedings of the 4th Int Conf AES 2004, pp. 27–41, 2004

[13] D. Mukhopadhyay, “An improved fault based attack of the advanced encryption standard,” Lect. Notes Comput. Sci. (including Subser. Lect.Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 5580, pp. 421–434, 2009.

[14] C. H. Kim, “Diferential fault analysis against AES-192 and AES256 with minimal faults,” in Proceedings of the 7th International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2010, pp. 3–9, USA, August 2010.