ENRICHING AES THROUGH THE KEY GENERATION FROM GENETIC ALGORITHM

Pooja Bagane

Research Scholar, Visvesaraya Technological University, Belgaum, Karnataka- India. Assistant Professor at Department of Computer Science, Symbiosis Institute of Technology, (SIT) affiliated to Symbiosis International (Deemed University), Pune, India.
poojabagane@gmail.com

Dr. S. Kotrappa

Professor, Department of Computer Science & Engineering, KLE Dr. MSSCET, Belgaum, Karnataka- India.
Kotrappa06@gmail.com

Abstract

Data security and encryption is one of the most useful at highly essential aspects of enabling effective security of the data against attacks and intrusions. This is an effective and useful technique that has been evolved significantly over the past few years. For the purpose of encryption the DES was prominently used before. The data encryption standard is highly effective but was prone to encryption failure against brute force attacks that have been highly effective against this encryption standard. Therefore the advanced encryption standard has been used since then to improve the performance of encryption significantly. The advanced encryption standard has been useful and realization of effective security but has been optimized specifically for achieving high throughput and high bandwidth for a variety of implementations. In this methodology we propose an enhancement to the AES encryption approach through the improvement of key generation process through the utilization of the genetic algorithm. The effective and useful implementation of genetic algorithm has been significantly useful for improving the performance of the AES encryption considerably.

Keywords: **AES Encryption; Cryptography; Key Generation; Genetic Algorithm; Security.**

1. Introduction

With the rise information technology and the large amount of information being generated every day there is a need for an effective realization of a secure technique for safeguarding this information effectively. This information age has led to a lot of information explosion, which can be addressed as a large number of people have a lot of personally identifiable information about themselves such as bank accounts social media IDs corporate ID is along with various identification documents that need to be secured to prevent them from malpractice. In the event of a data leakage this can be a problematic scenario as it can be highly difficult to prevent any identity theft and other problems that can be significantly dangerous and lead to a lot of complications for the individuals.

There are various techniques that have been utilized for the purpose of securing the data effectively. The traditional techniques have been designed around preventing the access to the data for any random individual. Through this process the data is isolated effectively and any attacker cannot get access to this data due to it being extremely isolated. This technique is not effective for various other documents and information that needs to be shared with other individuals at the same time prevented from misuse. For this purpose, the encryption or cryptography is one of the most effective techniques that are utilized for safeguarding for securing the data with great security. The encryption standards or cryptography comes in various flavors according to the implementation and the various characteristics of the data.

These cryptographic approaches tend to modify the data effectively to prevent any misuse effective identification. Through the cryptographic process are generally identifiable data is converted into random characters through the process of encryption. Encryption is one of the two most important processes that are performed in cryptography for the purpose of effectively e transforming the representation of data from one structure to another unique structure. This makes it extremely difficult to identify what kind of information or data is there the attacker encrypts that; this allows the data to be effectively protected from the malicious users effectively.

But the data also needs to be utilized coherently by the receiver or should be in the readable form for the owner of the data at least. For this purpose, a decryption process is performed which effectively transforms the data from its encrypted cipher text into the normal text that was originally utilized for the encryption process. Which is the other and the most important half of the cryptographic process which restore the original data which that can be utilized effectively for whatever purpose the data is being used. This entire approach is formed due to these two main procedures of cryptography and there are a number of different algorithms that are being used for the purpose of achieving this approach.

The data encryption standard was on the first and widely used techniques for the purpose of encryption to safeguard the data from data leaks. This is highly effective and was utilized for a long time before certain vulnerabilities we noticed in this encryption standard. The data encryption standard was highly susceptible to brute force attacks that could break into such algorithms and arrival the secure cipher text and convert it into the plaintext effectively compromising the data. For this purpose, the data encryption standard which is highly uncertain was dropped altogether and a new approach called the advanced encryption standard supported by Rijndael algorithm was utilized. This continues to be the most secure and an industry standard that is being utilized for the purpose of achieving cryptography by the National institute of standards and technology. These are effectively used in implementing cryptography in a lot of different approaches such as service cellular phones from where is firewalls etc.

But there are certain influences that have been significant in achieving the implementation of AES as we see today. The AES implementations normally for improving the security of where is implementation concentrates on achieving high throughput. This is due to the fact that most of these implementations do not have extensive computational capabilities to achieve complicated calculations easily. Therefore, for this purpose a lot of field gate programmable arrange are used is the can be effectively useful for providing physical security to the devices as well as improve the agility of the algorithm. The height of food is highly useful as it supports incredible security and also realizes a high bandwidth that can be effective for a variety of applications.

Section 2 of this research paper concentrates on elaborating the state of the art in the field. Section 3 of the proposed methodology explains the detailing of the implementation. Section 4 discusses the obtained result under the tag results and discussions. And finally, the section 5 concludes this research article along with the future enhancement scope.

2. Literature Review

K. Sandyarani states that in there has been an increase in the need for security of various implementations due to a large number of threats being perceived. This paper outlines an effective technique for the purpose of enabling Advanced Encryption Standard in the satellites for easier and safer encryptions of the data being transmitted [1]. The data being transported from the satellite is highly valuable and confidential therefore; this approach effectively makes it a secure and highly useful approach for protecting the data.

Fang Rao explains that there has been an increase in the energy consumption in devices which is problematic to achieve effective and accurate encryption. This paper discusses the consumption of energy and the effective utilization of encryption protocols in devices with limited power [2]. The authors state that an effective energy efficient technique needs to be implemented for the purpose of achieving encryption on the ZigBee network. For this purpose and AES algorithm has been revised and an effective encryption has been achieved on limited energy consumption.

Sandhya Koteshwara expresses that there is a need for an effective approach to secure shared messages. This research article the authors have elaborated on the topic of authenticated encryption that effectively maintains the integrity of the shared message along with the confidentiality intact [3]. They have been various approaches that have been utilized to achieve this technique but most of them have not been as effective in their implementation. Therefore, to improve the authors of proposed utilization of advanced encryption standard along with issuance resistance for achieving effective authenticated encryption that can be applicable on FPGA platforms.

Ritambhara elaborates on the growing number of internet of things devices which need effective security for the data [4]. In this paper the authors discuss about encryption standards that are being utilized for securing the data and transferring. This is due to the fact that in this information is there is an increase in the amount of data that is being generated and shared with one another over vast networks. Therefore, for this purpose the authors have proposed an enhanced algorithm for implementing advanced encryption standard that utilizes cascading method for securing internet of things devices.

Chong Hee Kim discusses the use of minimal faults in the encryption of the data that can be highly useful in achieving an improvement. In this publication the authors have proposed the framework of encryption through advanced encryption standard. The AES is being used extensively for the purpose of achieving all-round security and protection of the data [5]. But there is a lack of effective analysis of differential fault in AES 256 and AES 192. Therefore, this research article focuses on achieving the minimal faults in the advanced encryption standard implementation.

Noemie Floissac introduces the concept of providing effective security an encryption to the data for the purpose of achieving an analysis of the differential fault in the encryption procedure [6]. The advanced encryption standard has been effectively elaborated for the purpose of identifying the differential fault and effectively analyzing it from an attack point of view. The authors have attack the AES encryption standard through injection of faults and analysis of the same extensively.

Feng-Hsiag Hsiao discusses the approach of achieving an effective improvement in the encryption approach which can significantly improve the performance and the implementation goals [7]. The advanced encryption standard has been analyzed in this research article for the purpose of improving the efficiency and implementation in chaotic synchronization systems. This type of systems is not as effective for advanced encryption standard therefore the authors have improved this approach through the utilization of an auxiliary consisting of the genetic algorithm.

Aura Conci states that there has been an increased interest in the paradigm of cryptography for the purpose of achieving security for the data in various scenarios. The authors in this approach have analyzed steganography techniques on color images through the utilization of the advanced encryption standard [8]. The advanced encryption standard is highly difficult to achieve cryptography in the images therefore the authors and proposed the utilization of the genetic algorithm to achieve the goal.

Rodrigo S. Semente explains that there have been a large number of cryptography approaches that have been analyzed for the purpose of achieving an effective improvement in the security of the data. The authors in this paper have analyzed a large number of encryption techniques for the purpose of implementation in constant environments such as wireless sensor networks [9]. Most of the approaches have not been able to effectively achieve security as well as maintain the efficiency of the low power systems in the wireless sensor networks. The effort to improve this approach the authors of proposed the implementation of genetic programming for achieving a highly efficient cryptography for wireless sensor networks.

Avinash Ray elaborates on the paradigm of watermarking to improve the security of an image effectively. In this research article the authors have effectively analyzed the implementation of various encryption protocols for the purpose of watermarking and achieving image encryption [10]. The authors have compared XOR operation, affine transform, genetic, RSA and AES cryptographic techniques for the study.

Takeshi Tsujimura expresses that there has been an increase in the number of effective realization for the purpose of enabling effective gesture recognition [11]. This research article deals with the effective collection of finger science data through electromyogram sensors for the purpose of gesture detection. The authors have implemented genetic reasoning to identify the finger signals accurately through the electromyogram data.

V. Ten introduces the concept for the purpose of achieving an effective methodology of a hybrid approach for energy generation and the effective security of the data being generated in these facilities [12]. The research article in this approach has been analyzed for the purpose of implementing a renewable and hybrid power system based on wind, water and solar combinations. The authors and effectively utilize genetic algorithm to solve the optimization problem for achieving additional equilibrium in the hybrid power system.

K. Kalaiselvi discusses the concept of achieving robust and secure communication to achieve an effective improvement in this paradigm through the implementation of accurate encryption [13]. This research article defines an effective approach for the purpose of achieving secure communication and data transfer through the use of cryptography. The authors in this research are proposed an improved AES algorithm through the use of neural networks and genetic algorithm.

Dr. R. V. Kshirsagar narrates that the paradigm of cryptography is one of the most effective and useful implementations for the purpose of achieving an effective improvement in the security of data especially in low power devices. In this research article the authors have effectively proposed accept or graphics keep for the purpose of achieving secure services for various implementations where low power consumption is required [14]. The photo achieves their goals the authors have implemented very large scale infrastructure along with field programmable gate arrays to achieve advanced encryption standard.

Thanapol Hongsongkiat states that there has been an increase in the number of attacks on data that is being stored on low power devices which needs to be accurately safeguarded [15]. The researches in this research article have proposed an effective enhancement in the advanced encryption standard for the purpose of being implemented on CMOS architecture. This implementation has been achieved AES and encryption for RFID tags through the use of appropriate software and hardware.

3. Proposed Methodology

The steps that are encountered in implementing of the Advanced Encryption Standard algorithm along with the key generation using the genetic algorithm are depicted in the above figure. And the steps that are included in this process are explained in details with the below mentioned steps.

Step1 : Key generation through Genetic Algorithm: To generate a key for encryption using AES algorithm a current time instance is considered as the initial population. This time instance contains date, month,year,hour,minute ans second attributes. These attributes are concatenated into a string and fed to the MD5 hashing algorithm to generate a 32-character hash keys. This 32-character hash key is used to cross over to the modulus operation for the required number of key characters.

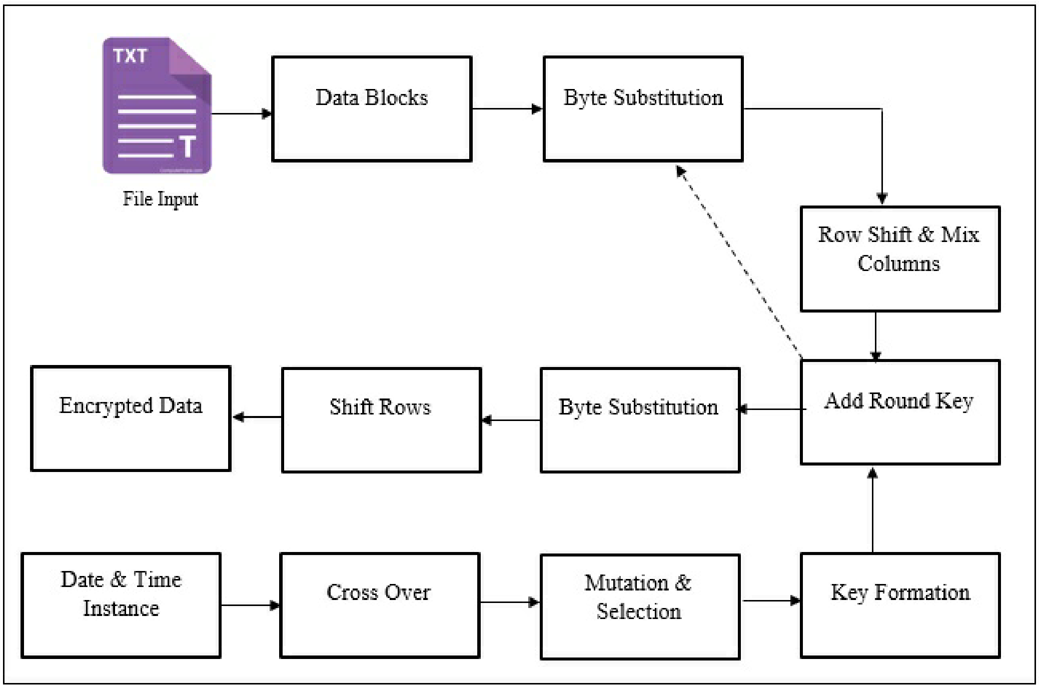

Fig. 1. System Overview

Based on this crossover a mutation of the key characters is done based on the rotation of the key stored in an array. Then, based on this mutation right fitting key characters are being selected and concatenated to the empty key string assigned at the beginning. This generated key is set the size of 8 characters and is used for the AES encryption process. The key generation model can be depicted in the algorithm 1 as mentioned below.

Algorithm 1: Keg Generation through Genetic Algorithm

```
// Input :  Instance data and time String $DT_{STR}$
// Output : Secure  Key $S_{KEY}$
Function : KeyGenerator($D_{STR}$ )
Start
$S_{KEY}$ =Ø
HashKey $H_{KEY}$=MD5 ($D_{STR}$)
      N=$H_{KEY}$ MOD  8
   If  N<8, then
   P=N+1
     for  i=0 to $S_{KEY}$ length < 8
          i=i+P
         if  i < $H_{KEY}$ length, then
         $S_{KEY}$= $S_{KEY}$+ $H_{KEY}$ [i]
         $H_{KEY}$ =rotate($H_{KEY}$ )
         end if
         else
         i=0
    end For
    end if
return $S_{KEY}$
Stop
```

Step 2: Data Block and Byte Substitution – The fed file is read into the byte array and then, this byte array is divided into blocks of 128 bytes. The last block is padded to equalize the size of the 128 bytes, so that all blocks are maintained equally. These blocks of the bytes are stored in an array to substitute according to the Exclusive OR operation mode. Then this data is framed into a matrix of 4 X 4, which is called state array.

Step 3: Row Shifting and mixing column: Now the obtained state array in the previous step is subjected to shifting of the rows and mixing of the columns for the given number of the rounds. For each of the iterations the key which is generated through genetic algorithm is weaved into the byte substitution process to obtain the tough cipher text. This process of AES structure can be pictorially shown in below figure 2.

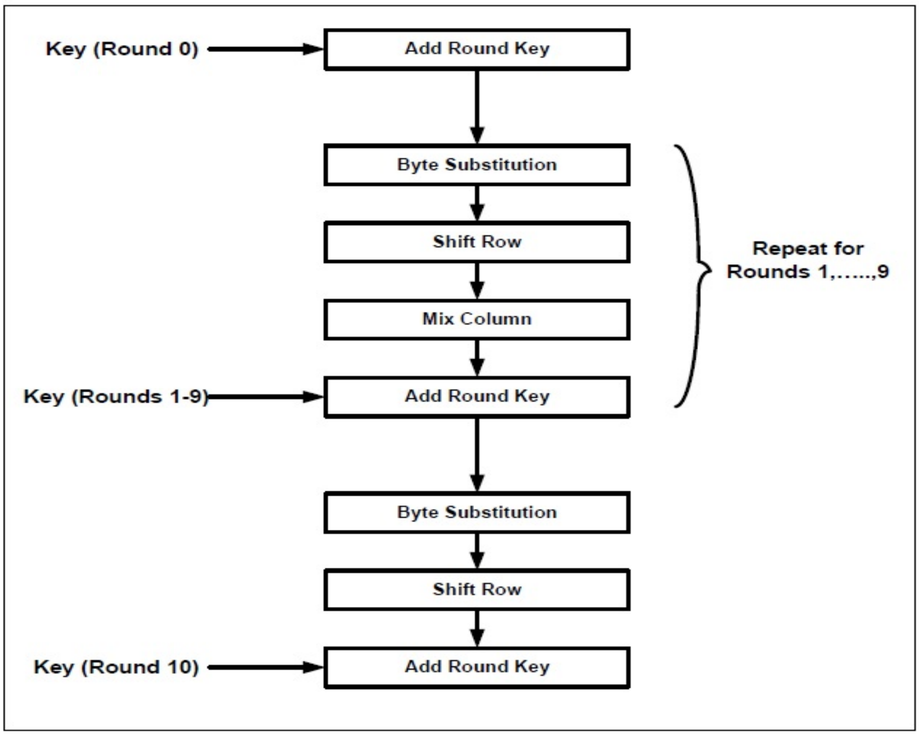

Fig. 2. AES Structure

Step 4: Byte Substitution and Shift Rows: This is the last step of the AES Encryption where shifted array after many rounds is subjected to the substitution of the other bytes based on the position and finally the rows are again shifted from the 4 X 4 matrix. After this process all the bytes are concatenated to obtain a single byte array to convert this into a string. The obtained string will cipher text for the given input data.

4. Results and discussion

The proposed methodology for achieving effective and useful key generation in advanced encryption standard through the use of the genetic algorithm has been effectively deployed through the utilization of Java programming language. The system has been achieved an integrated development environment of NetBeans 8.2 on a laptop running on an Intel core i5 processor assisted with 500 GB of hard drive and 4GB of RAM. The MySQL database server is utilized for fulfilling the data management and storage responsibilities.

The proposed methodology has been evaluated through extensive experimentation performed to achieve the performance metrics. Experimentation procedure has been detail effectively in the section given below.

Key complexity

To effectively determine the evaluation of the procedure we have try to understand the complexity of the key that is being generated by the genetic algorithm approach. Evaluation has been performed through the determination of the number of instances that are created during execution of the system and counting the respective number of keys for each of the instances. These values imported on a graph displayed in the figure 3 given below.

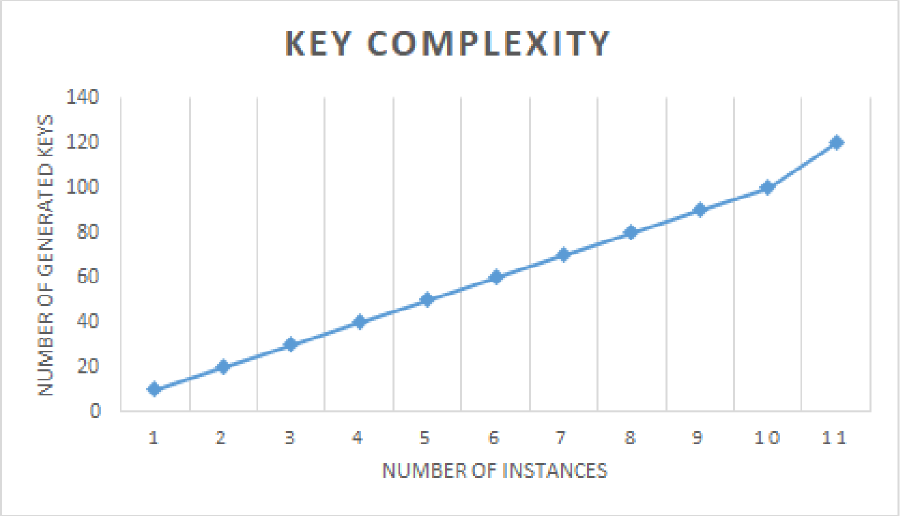

Fig. 3: Key Complexity

As it is evident from the above figure that the number of keys generated are dependent on the quantity of the instances in the proposed system. Therefore, this graph undeniably demonstrates and effective execution for model for key generation through the genetic approach.

Key space complexity

Another performance metric that determines the space complexity of the system for key generation through genetic algorithm on advanced encryption standard is the key space complexity. This type of complexity is highly useful in determining the amount of space that is allotted for the keys that are produced in accordance to the number of instances generated by the system. These keys are limited to 8 characters in length. As each character consists of 2 bytes each key generated through or proposed methodology takes up space of 16 bytes. This is consistent with the number of instances that are utilized in our approach as the number of instances are directly proportional to the space required for storing those keys. This can be effectively demonstrated through a graph given in figure 4 below.

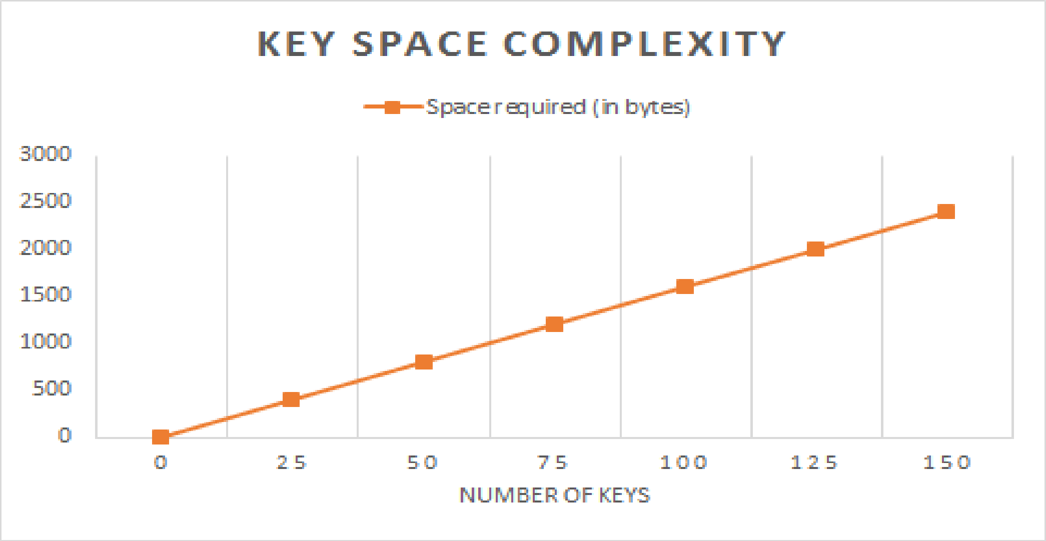

Fig. 4: Key Space Complexity Analysis

Character assignment for encryption comparison

The approach is further tested for the purpose of character assignment of the advanced encryption standard procedure for the key generation. The advanced encryption standard is one of the most effective approaches that utilizes symmetric encryption that is highly useful for the purpose of encryption and decryption with the same key.

The AES encryption procedure is put under the hammer for the purpose of determining the performance of the approach through the number of characters utilized for the purpose of achieving effective encryption. This is due to the fact that as the number of unique characters' increases in the key this leads to better performance of the encryption and significant improvement in the security of the data being encrypted. Therefore, the advanced encryption standard implemented in the proposed methodology is effectively experimented on for a number of experiments for the purpose of determining the number of different characters being utilized for the purpose of encryption for a given number of input characters.

The values achieved for this evaluation of the encryption technique is tabulated in the table 1 given below. These values are also contrasted with the encryption approach defined in [16]. Both of these values are effectively tabulated and the corresponding graph for comparison is being plotted in the figure 5 given below.

Experiment no.	No. of characters	No. of different characters (AES + GA)	No. of different characters (RCC)
1	0	0	0
2	1000	52	46
3	2000	58	52
4	3000	59	57
5	4000	62	55
6	5000	65	59

Table 1: Number of characters utilized for encryption (AES+GA v/s RCC)

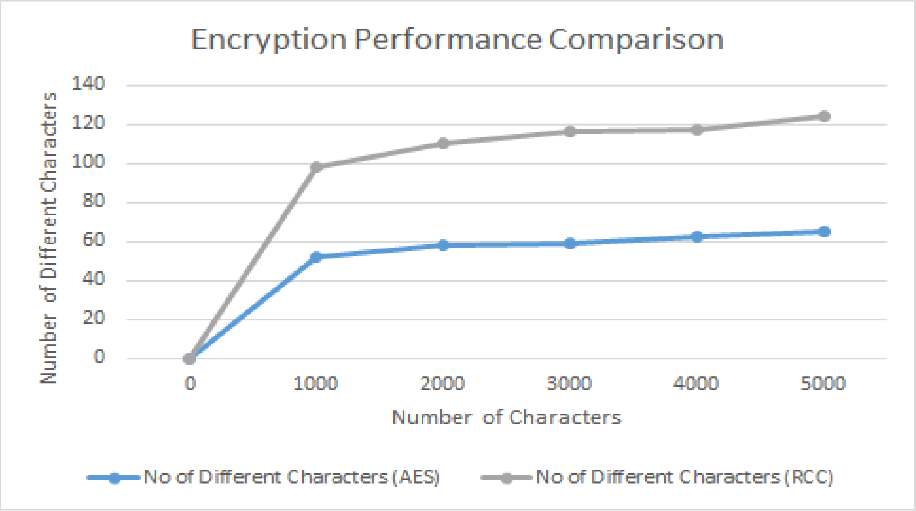

Fig. 5: Plot of the number of characters utilized for encryption in AES + GA v/s RCC encryption techniques.

As it is evident from the graph given in figure 2 the advanced encryption standard proposed in this approach is significantly better than the technique illustrated in [16]. This can be said with greater certainty due to the fact that the amount of different characters being utilized for the proposed advanced encryption standard approach is considerably more than the number of unique characters utilized for RCC encryption in the approach defined in [16]. The improved security and robustness of the advanced encryption standard gives it an edge which makes it difficult to be attacked or unrivalled easily leading to better security.

5. Conclusions

The methodology for the improvement of the key generation approach in the advanced encryption standard has been proposed in this research article. For the major encryption tasks the utilization of advanced encryption standard has been effectively realized through the National institute of standards and technology. The AES encryption standard utilizes different key sizes for the purpose of securing data these key sizes range from 256 192 and 128. This key sizes have been highly effective in realizing effective security through the use of field programmable gate arrays that provide effective security and agility to the algorithm which improves the performance. Moreover, the advanced encryption standard has been modified to achieve high throughput and bandwidth for implementation in a large variety of applications. In this research article this has effectively improved through the use of genetic algorithm that implements various elements such as mutation crossover selection to achieve key generation that satisfies the implementation effectively. This approach has been qualified through the use of extensive experimentation to achieve significant improvements over the conventional Rijndael algorithm approach.

In the future, this research can be extended to work as the readymade API that can be help to future developers to integrate the module into their software and also can be made to work on big data from cloud.

References

[1] K. Sandyarani and P. N. Kumar. (2013): Design and analysis of AES-CM with non-linearity S-box architecture. International Conference on Current Trends in Engineering and Technology (ICCTET), pp. 252-254, doi: 10.1109/ICCTET.2013.6675960.

[2] Fang Rao and Jianjun Tan. (2014): Energy consumption research of AES encryption algorithm in ZigBee. International Conference on Cyberspace Technology (CCT 2014) pp. 1-6, doi: 10.1049/cp.2014.1330.

[3] S. Koteshwara, A. Das and K. K. Parhi. (2017): Performance comparison of AES-GCM-SIV and AES-GCM algorithms for authenticated encryption on FPGA platforms. 51st Asilomar Conference on Signals, Systems, and Computers, pp. 1331-1336, doi: 10.1109/ACSSC.2017.8335570.

[4] Ritambhara, A. Gupta and M. Jaiswal. (2017): An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IOT). 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 422-427, doi: 10.1109/CCAA.2017.8229877.

[5] C. H. Kim. (2010): Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults. Workshop on Fault Diagnosis and Tolerance in Cryptography, pp. 3-9, doi: 10.1109/FDTC.2010.10.

[6] N. Floissac and Y. L'Hyver. (2011): From AES-128 to AES-192 and AES-256, How to Adapt Differential Fault Analysis Attacks on Key Expansion. Workshop on Fault Diagnosis and Tolerance in Cryptography, pp. 43-53, doi: 10.1109/FDTC.2011.15.

[7] F. Hsiao and G. Liou. (2014): Application of Advanced Encryption Standard to Chaotic Synchronization Systems: Using an Improved Genetic Algorithm as Auxiliary. International Conference on IT Convergence and Security (ICITCS), pp. 1-4, doi: 10.1109/ICITCS.2014.7021740.

[8] A. Conci, A. L. Brazil, S. B. L. Ferreira and T. MacHenry. (2015): AES cryptography in color image steganography by genetic algorithms. IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pp. 1-8, doi: 10.1109/AICCSA.2015.7507100.

[9] R. S. Semente, A. O. Salazar and F. D. M. Oliveira. (2014): CRYSEED: An automatic 8-bit cryptographic algorithm developed with genetic programming. IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, pp. 1065-1068, doi: 10.1109/I2MTC.2014.6860905.

[10] A. Ray, A. Potnis, P. Dwivedy, S. Soofi and U. Bhade. (2017): Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption. International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE), pp. 274-278, doi: 10.1109/RISE.2017.8378166.

[11] T. Tsujimura, T. Hashimoto and K. Izumi. (2014): Genetic reasoning for finger sign identification based on forearm electromyogram. International Conference on Applied Electronics, pp. 297-302, doi: 10.1109/AE.2014.7011724.

[12] V. Ten, B. Matkarimov and N. Isembergenov. (2013): Approach to Control of Hybrid Renewable Power System on the Basis of AE-Method Using Genetic Algorithm. 12th International Conference on Machine Learning and Applications, pp. 199-202, doi: 10.1109/ICMLA.2013.123.

[13] K. Kalaiselvi and A. Kumar. (2016): Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box. IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), pp. 1-6, doi: 10.1109/ICCTAC.2016.7567340.

[14] R. V. Kshirsagar and M. V. Vyawahare. (2012): FPGA Implementation of High Speed VLSI Architectures for AES Algorithm. Fifth International Conference on Emerging Trends in Engineering and Technology, pp. 239-242, doi: 10.1109/ICETET.2012.53.

[15] T. Hongsongkiat and P. Chongstitvatana. (2014):AES implementation for RFID Tags: The hardware and software approaches. International Computer Science and Engineering Conference (ICSEC), pp. 118-123, doi: 10.1109/ICSEC.2014.6978180.

[16] Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi. (2013): Reverse Circle Cipher for Personal and Network Security. International Conference on Information Communication and Embedded Systems (ICICES).

[17] Pooja Bagane and Dr. K. V. Kulhalli. (2015): Genetic Algorithm for Cryptography. International Journal of Computer Application Issue 5, Volume 1.

[18] Pooja Bagane and Kotrappa Sirbi. (2016): Cryptanalysis for S-DES using Genetic Algorithm. International Conference on Smart Electronic Systems (ICSES 2016) and published in International Journal of Technology and Science, Volume – 9, issue 2.

[19] Pooja Bagane and Dr. Kotrappa Sirbi. (2020): Bibliometric Survey for Cryptanalysis of Block Ciphers towards Cyber Security. Library Philosophy and Practice.

[20] Pooja Bagane and Dr. Kotrappa Sirbi. (2021): Comparison between traditional cryptographic methods and genetic algorithm based method towards Cyber Security. International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 12, Issue 2, pp. 676-682.

[21] Goldberg, D. E. (2009): Genetic Algorithms in Search, Optimization, and Machine Learning. Pearson Education, Fourth Edition.

[22] Rahman Dalimunthe, A., Mawengkang, H., Suwilo, S., Nazam, A. (2019): Vernam Cipher with Complement Method and Optimization Key with Genetic Algorithm. Journal of Physics: Conference Series.

[23] Pujari, S.K., Bhattacharjee, G., Bhoi, S. (2018): A Hybridized Model for Image Encryption through Genetic Algorithm and DNA Sequence. Procedia Computer Science.

[24] Sen, A., Ghosh, A., Nath, A. (2017): Bit level symmetric key cryptography using genetic algorithm. Proceedings - 7th International Conference on Communication Systems and Network Technologies, CSNT 2017.

[25] Farhat Ullah Khan, Surbhi Bhatia. (2012): A NOVEL APPROACH TO GENETIC ALGORITHM BASED CRYPTOGRAPHY. International Journal of Research in Computer Science, ISSN 2249-8265 Volume 2 Issue 3 pp. 7-10.

Authors Profile

Pooja Bagane, Research Scholar in Visvesaraya Technological University, Belgaum, Karnataka- India and also working as an Assistant Professor at Department of Computer Science, Symbiosis Institute of Technology, (SIT) affiliated to Symbiosis International (Deemed University), Pune, India. She has completed M.Tech. in CSE with Gold Medal. She was an academic topper throughout the years. She has published manuscripts in reputed journals. Her research, primarily in security, evolutionary algorithms, artificial intelligence & Machine Learning, and genetic algorithms.

Dr Kotrappa Sirbi, Professor in Computer Science and Engineering, qualification (B.E, M.S, M Tech, PhD), having 32 yrs experience in teaching and research. He has published over 50+ manuscripts, including journal articles. His research, primarily in data science, security, artificial intelligence & Machine Learning, and software engineering. He has Guest Edited several journal special issues. He has served on several editorial review boards.