# Securing Medical Text Data using Cuckoo Search based Advanced Encryption Standard (AES)

Dr. Gnanaprakasam Thangavel[1], Tigist Adam[2]
*[1](Assistant Professor/Department of Computer Science, College of Computing, Debre Berhan University, Ethiopia)*
*[2](Dean/Department of Information Technology, College of Computing, Debre Berhan University, Ethiopia)*
*Corresponding Author: Dr. Gnanaprakasam Thangavel*

***Abstract:****The internet plays vital role in the current digital era. The growth of the internet makes more advancement in all the fields including virtual medical treatment, online medical prescription and even online medical supply. But the security needs more strong environments especially for medical data processing. Cuckoo Search Algorithm (CSA) provides feasible support to identify the powerful key for the purpose of encryption and decryption. In particular, online medical prescription is in the form of text data. Hence, Advanced Encryption Standard (AES) algorithm will provide more security rather than other algorithms. The cloud simulator is used to check efficiencies of encryption and decryption time. Different text files with varying sizes are used for performance comparison.*

***Keywords:*** *Advanced Encryption Standard, Cuckoo Search Algorithm, Decryption, Encryption, Medical Data.*

---

Date of Submission: 18-11-2018 Date of acceptance: 04-12-2018

---

## I. Introduction

The word 'Smart' makes human life very smart. Usage of smart phones massively increased in all over the world. E-Health and Tele-Medicine schemes invented to save the time where they spend with hospital environment. Medical related data are harder to maintain, so the Medical Big Data (MBD) is useful at this scenario [1]. The sensitive information stored in the public environment is challenging task. It is very important that the accuracy and standard of the data which maintained in the hospital database should be secured. MOOC (Massively Online Open Course) was introduced to provide the necessary training to the persons who are handling the data [2]. A lot of challenges entered to maintain the sensitive information in public environment. AES provide the encryption and decryption. The smart phone world connects the smart devices like embedded sensors, mobile devices, IP phones, IP devices and software [3]. The digital communications between the devices are quite easy, but the security is the difficult measure. AES takes the leading role to provide the strong security with IoT devices [3]. The complex problems are solved with CSA [4]. Cuckoo Search invented in 2009 by Yang and Deb. The strong key will be identified through CSA and that will be used in AES algorithm. AES is more suitable for the text encryption process.

## II. Literature Survey

### 2.1 Survey about Medical Data:

E-Health and Tele-Medicine processes are massively increased in this smart devices world. Fadia Shah et al. (2017) started the research about E-Health and Tele-Medicine. The research focused more about prescription reports in text form, test reports, X-Ray and CT scan data. Finally, the team developed the Medical Big Data to store all the types of data and used for future reference purposes. Wang Xinyan et al. (2015) planned the new concept MOOC to train the people who involves in the core part of the data storage. Blood Pressure (BP) is the key disease of their main proposal; the team developed a prototype in which the patients who are in need can get the BP data immediately.

### 2.2 Survey about Cuckoo Search Algorithm:

Mareli et al. (2018) proposed that, optimisation problems are easily solved by cuckoo search. In the research proposal, mathematical test functions are used to verify the test results. That research simulation results confirmed that, more optimization problems are easily solved by cuckoo search. Mana Sopa et al. (2016) checked the reliability of the cuckoo search algorithm, which focused towards the cost of the hardware to create the sub system. In 2018 Fu Gui-xia et al. proved with the visual tracking tool with the help of the cuckoo search algorithm. Particle filter based cuckoo search was used for visual tracking applications, experiments of the visual tracking proved the support of the cuckoo search. Cai Zefan et al. (2018) tried with bionic swarm optimization for the purpose of deep search. Through the experimental research, it was proved that, global search ability and also convergence speed are increased in the cuckoo search algorithm.

### 2.3 Survey about Advanced Encryption Standard:

The requirement of fast encryption for Graphics Processing Unit (GPU) brings the AES encryption scheme in 2010 by Fei shah et al. The experiment results shows that there are 128, 192, and 256 lengths of bits encryption methods and compared with the execution times. Ritambara et al. (2017) proposed 200 bit key encryption methods with the plain text data. They used the cascading techniques for AES encryption to overcome the complexity issues. Lokireddi Phani Kumar et al. (2016) tried the AES for the purpose of Speech Encryption. Digital information should be secured from the security threats are the main objective of their research. Authenticity and confidentiality are the 2 requirements of their proposal. Amal Joshy et al. (2018) achieved the text to image encryption with the help of the AES algorithm. They tried with RGB substitution technique method to store the images and for retrieval purposes.

## III. Proposed Methodology

### 3.1 Identify the Strong Key using CSA:

CSA is nature inspired algorithm. They are unique by obligate brood parasitism. The female cuckoo lays its egg in to the nest of other birds. The host bird never knows the brood parasitism of the cuckoo. This is nature’s play. From this, the followings assumptions will come.

a. The cuckoo lays only one egg (key) at a time into the random nest of host bird.
b. The best egg (strong key) from the quality nest will be forwarded to the next generation.
c. The host bird’s nest is fixed, and the host bird can discover the cuckoo’s egg with a probability.

3.1.1 CSA Steps

```
1. Generate Initial Population of n host bird nests $X_i$ ; $i = \{1,2,3….n\}$.
2. while (time < Max_Generation) or (Stop Criteria) do
        Get a cuckoo randomly by levy flights; evaluate quality/fitness $F_i$;
        Choose a host bird nests (j) randomly;
        if $F_i > F_j$ then
                replace (j) with new solution;
        (i)will be discarded and new ones are built;
        Keep the best solutions
3.Take the best solution
```

The above CSA algorithm is implemented with java language, and the best solution in the end is called shared secret key and it will be used in AES encryption and decryption process.

### 3.2 Securing the Data using AES:

AES is a symmetric algorithm; there is no need of private/public keys for the encryption/decryption. AES use only the shared secret key. In this research, the shared secret key is the output of CSA. AES is developed by Rijndael in the year 2001.

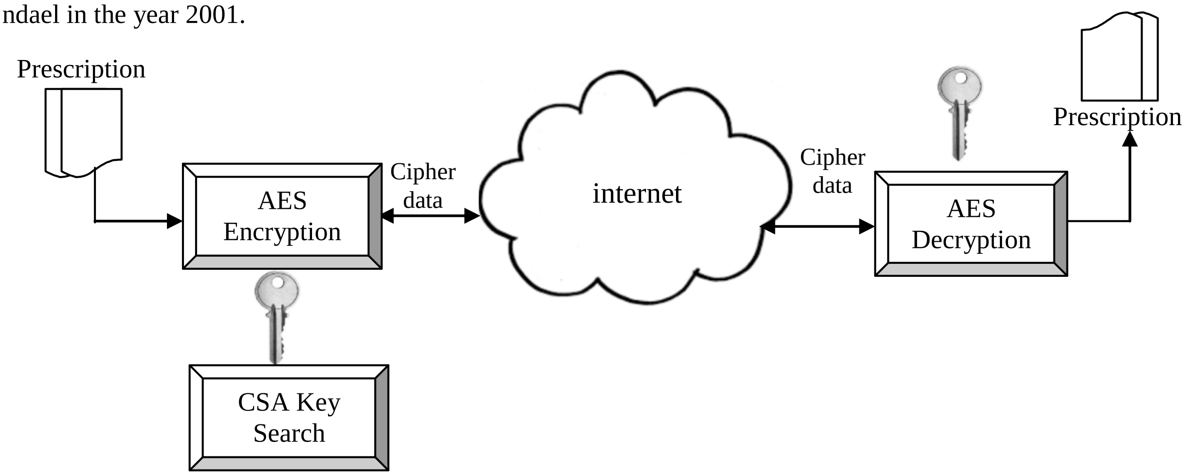


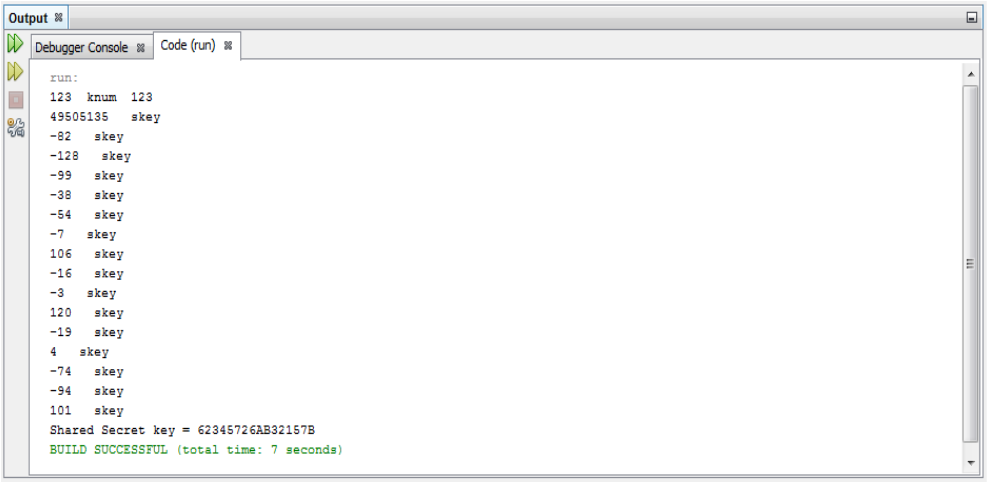
**Figure 3.1** Encryption and Decryption Process using AES.

The above FIGURE 3.1 is the proposed structure of the encryption and decryption process of the medical data. Prescription of the doctor is encrypted with the support of shared secret key which is generated from the cuckoo search algorithm. In the receiver (patient) end, using the shared secret key, patients can see the prescriptions of the doctor.

## IV. Implementation

### 4.1 CSA Key generation:

The CSA Key Generation is implemented with jdk8.1 compiler. The key generation time may be varied depending upon the compiler, processing speed and operating system which is used by the user. The generated key will act as Shared Secret Key of the AES encryption and decryption. CSA's Shared Secret Key: 62345726AB32157B. It will be shared both sender (doctor) and the receiver (patient) objects respectively.

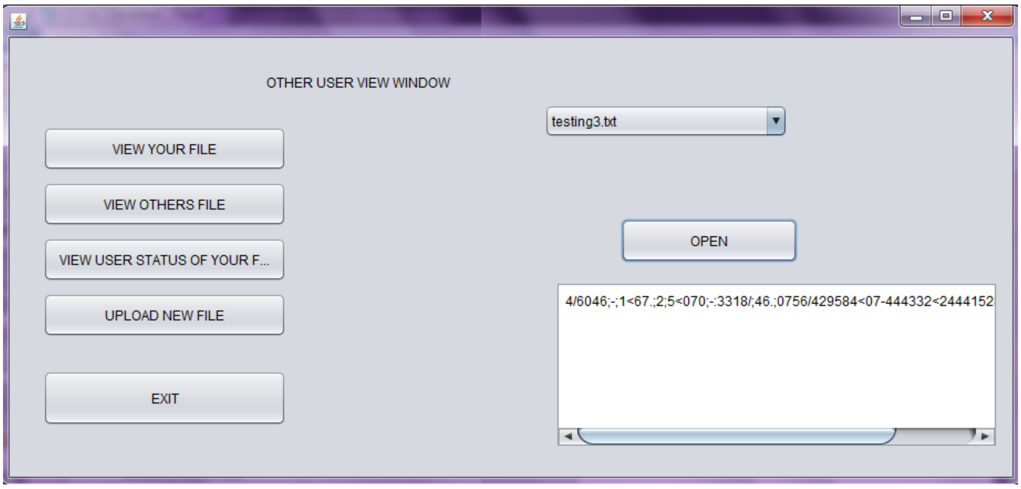


```
run:
123  knum  123
49505135   skey
-82   skey
-128   skey
-99   skey
-38   skey
-54   skey
-7   skey
106   skey
-16   skey
-3   skey
120   skey
-19   skey
4   skey
-74   skey
-94   skey
101   skey
Shared Secret key = 62345726AB32157B
BUILD SUCCESSFUL (total time: 7 seconds)
```

**Figure 4.1** CSA Key Generation.

### 4.2 AES Encryption Process of Prescription:

AES Encryption process is also implemented through jdk 8.1 compiler. After the encryption process the prescription (original message) will be converted as cipher text. Man in middle attack is not possible to capture the data and also without shared secret key none of the intruder can view the original message. The shared secret key will be given to each patient confidentially in order to maintain the security by default AES will provide the confidentiality and digital signature of the data.



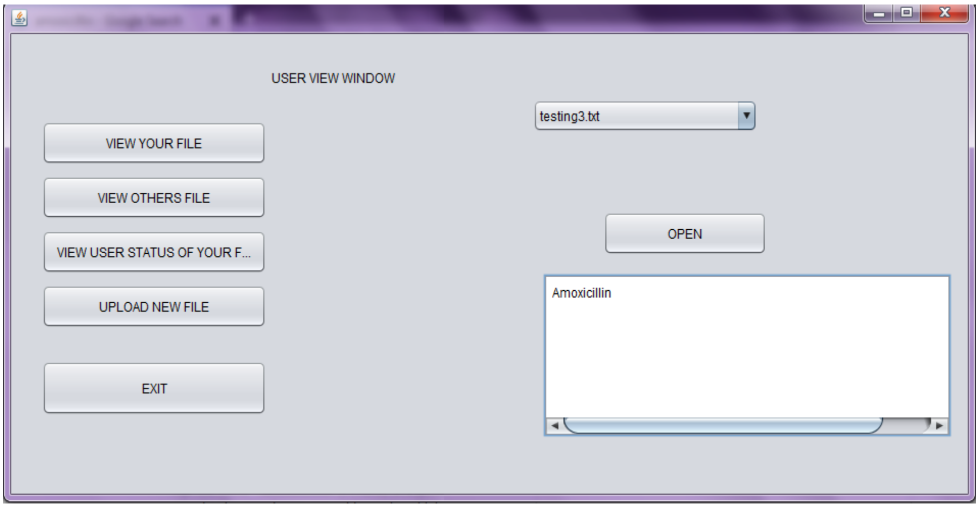
testing3.txt

4/6046;-;1<67.;2;5<070;-:3318/;46.;0756/429584<07-444332<2444152

**Figure 4.2** Encryption Process.

### 4.3 AES Decryption Process of Prescription:

AES decryption is in the users/patients end. The shared secret key is used to access the prescription of the doctor (original message). The other persons in the same system cannot view the original message of the doctor without the help of the shared secret key. The doctor sends the prescription (original message) along with the shared secret key. If a new shared secret key created for a particular patient the old key is not valid to decrypt the message. In this way, the data confidentiality is maintained with the medical text data.



testing3.txt

Amoxicillin

**Figure 4.3** Decryption process.

## V. Performance Analysis

Performance analysis of this proposed method is proved with two parameters respectively, processing time and information loss. In both scenarios, the text files (prescription) will be given as input and calculate the encryption time and decryption time. There is an extra processing time during encryption process because cuckoo search takes an additional time before encryption. This will be eliminated in decryption process.

### 5.1 Processing time:

Processing time means encryption and decryption times. There are different text files with various sizes are used to measure the performance of the AES algorithm.

**Table 5.1** Encryption and Decryption time

| File Size in KB | Encryption Time in ms | Decryption time in ms |
|---|---|---|
| 100 | 0.6 | 0.3 |
| 200 | 1.3 | 0.7 |
| 300 | 1.7 | 1.1 |
| 400 | 2.2 | 1.3 |
| 500 | 2.8 | 2.1 |

The above TABLE 5.1 shows the encryption and decryption processing times. With the above values the following graph proved the efficiencies.

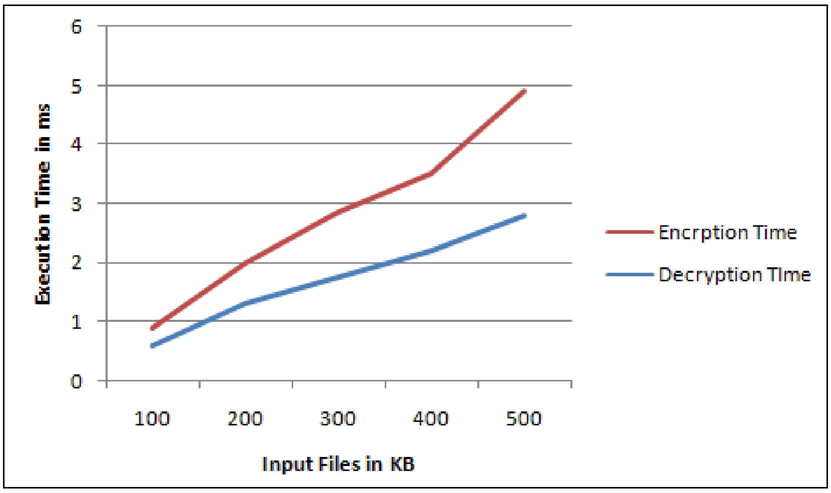


**Figure 5.1** Encryption time vs. Decryption time.

### 5.2 Information Loss:

The integrity of the original text (prescription) should not lose during encryption and decryption processes because all are medical data. So in this integrity testing, different files are checked with their cipher text and original text information before and after encryption. Table 5.2 indicates the different files after encryption and after decryption.

**Table 5.2** Original Message vs Encrypted Message.

| Original File Size in KB | Encrypted File size in KB | Decrypted File size in KB |
|---|---|---|
| 100 | 109 | 100 |
| 200 | 210 | 200 |
| 300 | 312 | 300 |
| 400 | 413 | 400 |
| 500 | 514 | 500 |

Though it is a text file, here is no loss in encryption and decryption files. Because it is a medical data, the loss should not be accepted even in 0.01% of data processing. The following graph illustrates there is no loss in encryption/decryption processes of AES processing.

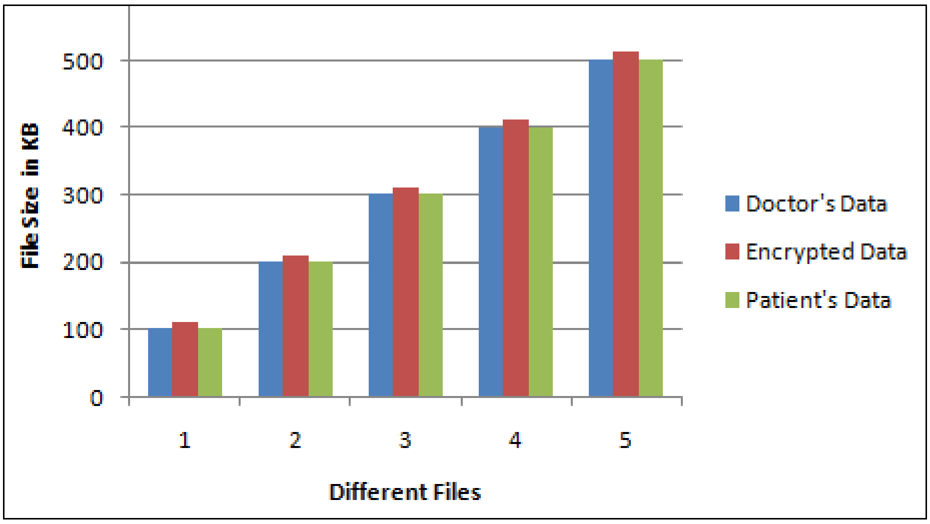


**Figure 5.2** Original prescriptions, Before and After Encryption.

## VI. Conclusion

Medical text data security is very essential in this digital threatening environment. This method showed that AES process increased the security feature in digital transmission of data. Cuckoo search algorithm improved the key strength of AES encryption and decryption. The performance comparison shows the efficiency of the encryption and decryption time. The proposed method proved that there is no information loss which increased the integrity of data transmission. Shared secret keys will be generated and always shared if there is a communication between the doctor and patient with respect to prescription transmission through online. In the future, the researchers can enhance this work with image data, because MRI, CT, and Ultra Sound scan outputs are in the form of images. Also, there is a possible with audio and video data processing because now the internet entered the rural villages.

## References

### Journal Papers:

[1] Fadia Shah, Jiaping Li, Raheel Ahmed Memon, Faiza Shah, Yasis Shah, Broad Big Data Domain via Medical Big Data, Proc. IEEE 14th International Computer Conference on Wavelet Active Media Technology and Information Processing, China, 2017, 327-331.

[2] Wang Xinyan, Tian Liyuan, Wu Wenjum, MOOC for Medical Big Data Research, Proc. IEEE First International Conference on Big Data Computing Service and Applications, California, 2015, 452-455.

[3] Arnab Rahman Chowdhury, Junayed Mahmud, Abu Raihan Mostofa Kamal, MAES: Modified Advanced Encryption Standard for Resource Constraint Environments, Proc. IEEE Sensors Application Symposium (SAS), South Korea, 2018, 140-146.

[4] Yang Xiaodong, Cai Zefan, Particle Swarm Optimization and Cuckoo Search Paralleled Algorithm, Proc. 3rd IEEE International Conference on Computer and Communications, China, 2017, 2236-2240.

[5] Amal Joshy, K X Amitha Baby, S Padma, K A Fasila, Text to image encryption technique using RGB substitution and AES, Proc. IEEE International Conference on Inventive Computing and Informatics (ICICI), 121-125, 2018.

[6] Rizky Riyaldhi, Rojali, Aditya Kurniawan, Improvement of Advanced Encryption Standard Algorithm with row and S.Box Modification Mapping in Mix Column, Proc. ScienceDirect, 2nd International Conference on Computer Science and Computational Intelligence, Indonesia, 2017, 401-407.

[7] Lokireddi Phani Kumar, A.K. Gupta, Implementation of Speech Encryption and Decryption using Advanced Encryption Standard, Proc. IEEE International Conference on Recent Trends in Electronics Information Communication Technology, India, 2016, 1497-1501.

[8] Ritambhara, Alka Gupta, Manjit Jaiswal, An Enhanced AES Algorithm using Cascading Method on 400bits key size used in Enhancing the safety of Next Generation Internet of Things (IoT), Proc. IEEE International Conference on Computing Communication and Automation, India, 2017, 422-427.

[9] Fei Shao, Zinan Chang, Yi Zhang, AES Encryption Algorithm based on the High Performance Computing of GPU, Proc. 2nd IEEE International Conference of Communication Software and Networks, China, 2010, 588-590.

[10] Flevina Jonese D'Souza, Dakshata Panchal, Advanced Encryption Standard (AES) Security enhancement using Hybrid Approach, Proc. IEEE International Conference on Computing, Communication and Automation, India, 2017, 647-652.

[11] M. Mareli, B. Twala, An Adaptive Cuckoo Search Algorithm for Optimisation, Journal of Applied Computing and Informatics, Vol.14, 2018, 107-115.

[12] Mana Sopa, Niwat Angkawisittpan, An Application of Cuckoo Search Algorithm for Series System with Cost and Multiple choices constraints, Proc. ScienceDirect International Electrical Engineering Congress, Thailand, 2016, 453-456.

[13] Fu Gui-Xia, Gao Ming-Liang, Zou Guo-Feng, An Improved particle filter based on Cuckoo Search for Visual tracking, Proc. IEEE Chinese Control and Decision Conference, China, 2018, 3687-3691.

[14] Mahbobe Bani Asad Askari, Mostafa Ghazizadeh Ahsaee, Bayesian Network Structure Learning based on Cuckoo Search Algorithm, Proc. IEEE 6th Iranian Joint Congress on Fuzzy and Intelligent Systems, Iran, 2018, 127-130.

[15] Cai Zefan, Yang Xiaodong, Cuckoo Search Algorithm with Deep Search, Proc. 3rd IEEE International Conference on Computer and Communications, China, 2017, 2241-2246.

Dr. Gnanaprakasam Thangavel. " Securing Medical Text Data using Cuckoo Search based Advanced Encryption Standard (AES)." IOSR Journal of Computer Engineering (IOSR-JCE) 20.6 (2018): 35-40.