Enhancing the Security for Clinical Document Architecture Generating System using AES Algorithm with Artificial Neural Network

[1]M·Sri Lakshmi, [2]Dr. B. Lalitha

[1]M. Tech Student, Department of CSE, JNTUA Engineering College, District Ananthapur, A.P, India
[2]Assistant Professor, Department of CSE, JNTUA Engineering College, District Ananthapur, A.P, India

---***---

ABSTRACT– *Electronic Health Record helps to improve the safety and satisfactory care of each patient details, which is important to be maintained by the medical institution, with the interoperability of Health Information Exchange (HIE).The CDA generation and integration system in cloud, uses open API to generate CDA files without purchase of proprietary software . Using CDA record integration system integrates multiple CDA documents of patient into a single CDA document. Both physicians and patient can make use of the scientific statistics in chronological order. In this paper, the CDA documents are combine into single record and may be browsed as a readable format. It is simple to examine and recognize for physicians correctly .The proposed work have been analyzed to verify the ability of ANN based key expansion to make the same cipher text as that accomplished by the conventional AES(Advanced Encryption Standard) for the same plain text. This model show the potential of the proposed work to produce the same secure system even with non-identical key expansion technique. However, the use of neural network adds more security to the conventional AES, because the adversary doesn't know the topology of neural network.*

Key Words: AES, ANN, Key Expansion, PRNG.

1. INTRODUCTION

Electronic Health Record (EHR) is longitudinal series of electronic fitness statistics of patients where health information is stored in the form of records. To access EHR in efficient way between the health information systems(HIS) one should maintain health information exchange(HIE). However, most of the Health information system provider have different characteristics and are together incompatible. Hence, a standardized health information exchange between hospitals needs to be implemented. Especially, medical report standardization lies at the core of guaranteeing interoperability. Health Level Seven(HL7) has established CDA for clinical documents which represents the structure and semantics of 'clinical documents' during exchange of documents. HL7 refer to a set of international standards for transfer clinical and administrative data between software applications used by various health care providers. The first version of CDA was introduced in 2001 and the later version came out in 2005. Many nations have adopted CDA for their projects. To establish self-assurance in HIE interoperability, more HIS's need to assist CDA. However, the structure of CDA may be very complicated and the production of correct CDA report is hard to gain without deep understanding of the CDA standard. In addition, the HIS improvement platforms for hospitals vary so significantly that generation of CDA files in every medical institution continually calls for a separate CDA generation. Also, hospitals are very reluctant to adopt new system unless it is in reality important for provision of care. As an end result, the adoption rate of EHR is very low in some nations like New Zealand or Australia. When the patient is recognized at a medical institution, a CDA file regarding the diagnosis is generated. The CDA report may be shared among different clinics if the patient doesn't have objection in sharing of his records. The idea of family doctor does no longer exist in Korea, it might common for a patient to go to some other clinics. The change of CDA report is brought on within the following cases: when a physician desires to study a patient's medical history. While a patient is in emergency and the scientific records wishes to be reviewed. It takes amount of time for the scientific personnel as the quantity of exchanged CDA record will increase due to having more documents allotted in distinct files. This considerably delay the medical personnel in taking decisions. Hence, when all the CDA documents are included into a single record, the clinical employees is empowered to check the patient diagnose history without difficulty in chronological order. Unfortunately integration of multiple CDA files into one, does not exist yet to the best of our knowledge.

2. RELATED WORK

Lee, S. H., Song, J. H., Kim, I. K., & Kim, J. W.[5],proposed CDA integration system and CDA integration template for HIES in Korea. As a physician spend limited time per patient in Korea this system will be useful for them. Kim, H. S., Tran, T., & Cho, H[6],proposed a next-generation hospital information system (HIS) based on the HL7 clinical document architecture (CDA) including in electronic health record (EHR) and a clinical data repository (CDR) to enable the sharing of medical information among health and medical institutions.

The existing system generates CDA based on cloud computing .This CDA generation and integration system works on different platforms as it makes use of an open API by which interoperability can be achieved. To analyze the working of existing system consider two hospitals A and B. In each hospital there will be HIS and CDA generation interface. With the help of this interface hospital A and hospital B will get CDA documents from the CDA generator API present in the cloud. CDA generator API makes use of the template manager[7] to generate Clinical documents in CDA standard[7] .The generated CDA will be validated against the CDA valuator that will give accurate CDA. Now this validated CDA will send back to the hospitals through CDA generation interface.

The existing system provides integration of CDA based on cloud computing. Each hospital will contain CDA integration API which is used to send the CDA documents to the cloud where different CDA documents of each patient will be integrated with the help of CDA parser and integrator.

This entire process of generation and integration of CDA performed in cloud not able to provide security to the CDA of patients. Hence, a cryptographic technique has been proposed in the present system. Security can be achieved by using AES with Feed forward network[5] in Artificial neural network.

3. PROPOSED WORK

AES is an iterated block cipher which takes a key length of 128 bits and it consist of 10 rounds for encrypting the data. In order to face the attacks a key expansion process was developed in AES. To provide more security[7] to the data, a neural network approach for the key expansion process in AES has been proposed in this paper.

Artificial neural network is an inspiration from biological nervous system, where millions of artificial neurons will be interconnected to each other in order to transfer data within fraction of seconds as does in human nervous system.

The neural network will take 4 words as input and takes initial weights with the help of PRNG (pseudo random number generator).This algorithm is for generating a sequence of numbers. The desired output given by neural network present in key schedule. We are comparing the target output denoted by X from training phase, with the output generated by NN denoted by Y, the difference between them is the error and the threshold value is set to 1.

Error = X-Y.

If the error is less than threshold value then output generated by the NN is considered as desired output. Otherwise we have to adjust the weights till we get error less than the threshold value. Like this keys will be extracted for encrypting and decrypting the data. The entire process is explained in the below fig1.

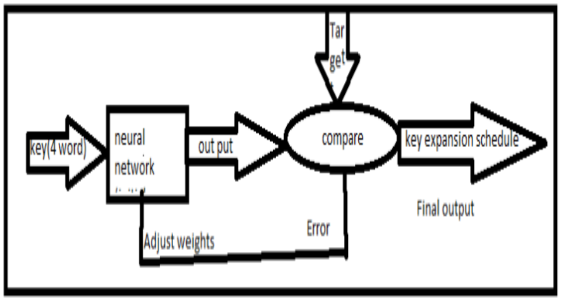


Fig1. Neural network key Expansion for encryption and decryption process.

In the training phase of the ANN, the AES algorithm generating the output from specific input the ANN takes the initial key (4 Word) as input and the key (40 Word) of the platform as output then the process will be terminated. The NN used in the training process has topology [4-4-40-1]. In other words , the neural networks consists of first layer with 4 neurons, second layer with 4 neurons, third layer with 40 neurons and the output layer contains only one neuron.

In training phase, a sigmoid activation function which is hyperbolic tangent on each neuron is implemented as given by the equation (1). AES takes the bits in the range of 0 to 255 where as the domain of sigmoid function is -1 to 1. In order to implement a neural network based AES the bits range should be taken from 0 to 1.

$$\tanh(\sum_{k=1}^{40} w_{1k}.\tanh(\sum_{k=1}^{40}\sum_{j=1}^{4} w_{kj}.\tanh(\sum_{j=1}^{4}\sum_{j=1}^{4} w_{ji}.\tanh(\sum_{i=1}^{4} w_{i1}.input)))) \text{ ----(1)}$$

sigmoid activation function

As AES takes 128 bit key hence the no of rounds will be ten where each round contains four steps. AES operates on a 4 ×4 matrix of bytes, called the state

AES Algorithm:

```
AddRoundKey(State,$key_0$)
for round=1 to Nr-1
{
    SubBytes(State,S-Box)
    ShiftRows(State)
    MixColumns(State)
    AddRoundKey(State,$Key_r$)
}
SubBytes(State)
ShiftRows(State)
AddRoundKey(State,$Key_{nr}$)
AddRoundKey(State,$Key_0$)
for round=Nr-1 to 1
{
    InvSubBytes(State,S-Box)
    InvShiftRows(State)
    InvMixColumns(State)
    AddRoundKey(State,$Key_r$)
}
InvSubBytes(State)
InvShiftRows(State)
AddRoundKey(State,$Key_{nr}$).
```

STEP-1: Sub Bytes

A nonlinear substitution step where each byte in the state is replaced by another one by using the Rijndael S-Box.[4].

STEP-2: Shift Row
A transposition step where the last three rows of state are shifted cyclically.

STEP-3: Mix Column
A mixing operation which operates on the columns of the state, it combines the four bytes in each column.

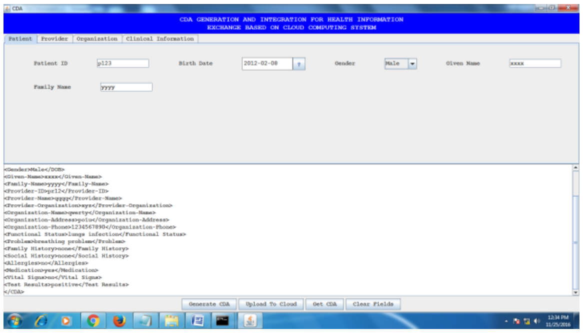
STEP-4: Add Round Key
Each byte of the state is combined with a round key, which is a Different key for each round and derived from NN key schedule.

For the tenth round step-3 will be omitted.
In Add Round operation, a key generated by neural network is applied to the state by a simple bitwise XOR. Hence security for CDA documents in cloud server is achieved through neural network based AES approach.

4. EXPERIMENTAL RESULTS

The proposed work observed by conducting different experiments.

Security to the CDA of patients achieved by giving access only to the authorized user. If an unauthorized user tries to access the data in CDA it will be appeared in encrypted format which is not readable for that person.

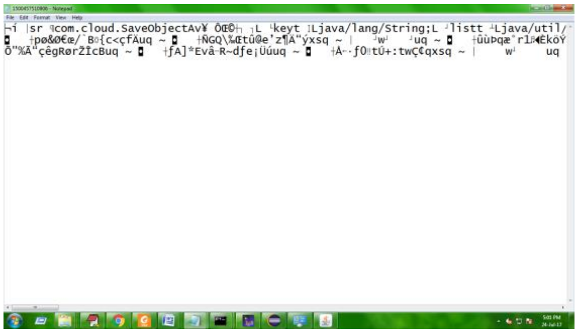


Patient ID p123
Birth Date 2012-02-08
Gender Male
Given Name xxxx
Family Name yyyy

```
<Gender>Male</DOB>
<Given-Name>xxxx</Given-Name>
<Family-Name>yyyy</Family-Name>
<Provider-ID>pr12</Provider-ID>
<Provider-Name>qqqq</Provider-Name>
<Provider-Organization>xyz</Provider-Organization>
<Organization-Name>qwerty</Organization-Name>
<Organization-Address>poiu</Organization-Address>
<Organization-Phone>1234567890</Organization-Phone>
<Functional Status>lungs infection</Functional Status>
<Problem>breathing problem</Problem>
<Family History>none</Family History>
<Social History>none</Social History>
<Allergies>no</Allergies>
<Medication>yes</Medication>
<Vital Signs>no</Vital Signs>
<Test Results>positive</Test Results>
</CDA>
```

Fig 1: CDA Generation and Integration system

Fig 1 shows the information provided by the authorized user such as patient name, provider details, organization and clinical information details.



```
┐í |sr ¶com.cloud.SaveObjectAv¥ ÕŒ©┤ ┐L ┘keyt ‖Ljava/lang/String;L ┘listt ┘Ljava/util/
◘   ┼pø&Ø€œ/ˆB□{c<çfÄuq ~ ◘   ┼ÑGQ\‰Œtû@e'z¶Ä"ýxsq ~ |   ┘w┘   ┘uq ~ ◘   ┼ûùÞqæ˚r1‼◄ÈköŸ
Õ"%Ä"çêgRørŽÎcBuq ~ ◘   ┼ƒA]*Evâ-R~dƒe¡Üúuq ~ ◘   ┼Å--ƒ0‼tÛ+:twÇ¢qxsq ~ |   w┘   uq
```

Fig2: Patient Data in Encrypted form

5. CONCLUSION

The proposed key generation method reduces the threats of breaking the symmetric keys by taking artificial neural networks and from it the overall key will be generated. This strengthen the security since ANN training used to obtain the round keys only known by sender and receiver, Neural cryptography is a division of cryptography devoted to evaluate the service of stochastic method, especially neural community algorithms, for use in encryption and cryptanalysis. Though nevertheless emerging, this branch of technological know-how gives safety to records transfer from one gadget to every other. Neural networks provide greater flexibility in securing cryptographic passwords as compared to the traditional techniques.

REFRENCES:

[1] T. Benson, Principles of Health Interoperability HL7 and SNOMED. New York, NY, USA: Spinger, 2009.

[2] S. R. Simon, R. Kaushal, P D. Cleary , C. A. Jenter, L. A. Volk, E. G. Poon, E. J. Orav, H. G. Lo, D. H. Williams, and D. W. Bates, "Correlates of electronic health record adoption in office practices : A statewide survey," J. Am. Med.Inform. Assoc., vol. 14, pp. 110–117, 2007.

[3] Fine, T. L. (2006). Feedforward neural network methodology. Springer Science & Business Media.

[4] K. Ashish, "Meaningful use of electronic health records the road a head, "JAMA, vol. 304, no. 10, pp. 1709–1710, 2010

[5]Lee, S. H., Song, J. H., Kim, I. K., & Kim, j. W.(2016). CDA integration system to support patient referral and reply letters. Health informatics journal, 22(2), 160-170.

[6]Kim, H. S., Tran, T.,& Cho, H. (2006, September).A CDA generate Clinical documents within a hospital information system for e-healthcare services. In Computer & Information Technology, 2006. CIT'06. The Sixth IEEE International Conference on(pp. 254-254). IEEE.

[7] B.lalitha,"Security & QOS cetric protocols for P2P networks : Current state of the art" vol 2, ISSN:2278-1323,2013.