International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Design Information Security System Using Elgamal With Ann Encryption

Harshada Sawant[1], Revati Salvekar[2]
Aishwarya Pandey[3,] Dipti Patil[4]

[1 2 3 4] *(Computer, JSPM's Rajarshi Shahu College of Engineering, India)*

Abstract :- By making use of AI, human-like intelligence can be enlivened by a machine; Neural Network is one of the subfield of AI. Artificial Neural Networks (ANN) are generally introduced as systems of interconnected neurons computing values from inputs. This project utilizes Hebbian learning rule to train the ANN of both sender and receiver machines. In Public key Cryptography(PKC),Pseudo Random Number Generator(PRNG) are extensively used to generate unique keys and random numbers used in ANN which are found to have many types of possible attacks. It is essential for a key to own randomness for key strength and security. This project put forward key generation for PKC by application of ANN using Genetic Algorithm (GA). It was observed that use of ANN along with GA has not yet been explored. GA is a very good challenger for PRNGs. GA PRNGs result samples fulfills frequency and gap test. Thus the numbers generated after each iteration by GA PRNG are demographically verified to be random and nonrepeating, acts as important initialization parameter for neural algorithm. Generating public and private keys through different rounds of mixing is used. Our algorithm was observed to give fast and enhanced performance results having practical and realizable implementation.

Keywords: - artificial neural networks, genetic algorithm, hebbian theory, public key cryptography, random number

I. INTRODUCTION

Cryptography is something which deals with encryption and decryption of data. It basically allows secure communication within insecure networks for e.g. Internet, E-mail Communication etc. Public Key Cryptography (PKC) uses public key for encryption and private key for decryption. A specific cipher text in cryptographic techniques is produced by a KEY. Sizes of keys are measured in bits as they are in large numbers. Cipher text is safer if we use large key but it gives slower encryption and decryption performance instead if we use small key it will give faster performance which includes little bit risk.

II. RELATED WORK

In concern with neural network the idea basically is like let's take an example suppose a person going for his office the way of going to the office is addressed in his mind so the person going to office will always follow the way he follows everyday even he has some different stuff in his mind. Artificial Neural Network (ANN) has showed a great contribution in treatment of patients with uninvestigated dyspepsia [1]. The concept which we are supposed to develop is shown in the figure 1.

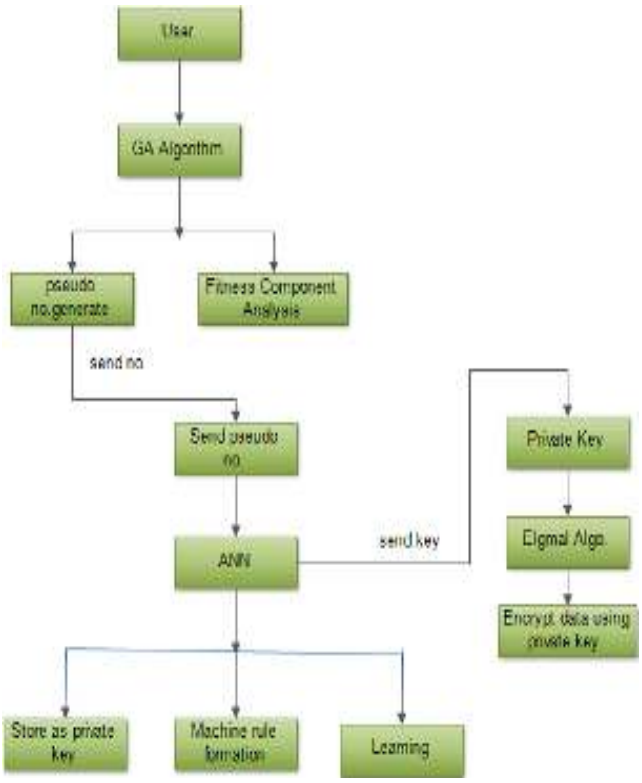

Fig.1. Flow Diagram of Proposed System

III. SYSTEM ARCHITECTURE

We have developed the architecture for such users those who wants the data as per their needs. The architecture consists such learning skills & learning objects using which the system can easily recommend the user for any learning object.

In the above system architecture shown in figure 2 the user needs to be register himself & while registration his complete profile will be created which includes his learning objects style & his level i.e. beginner, intermediate or any expertise.

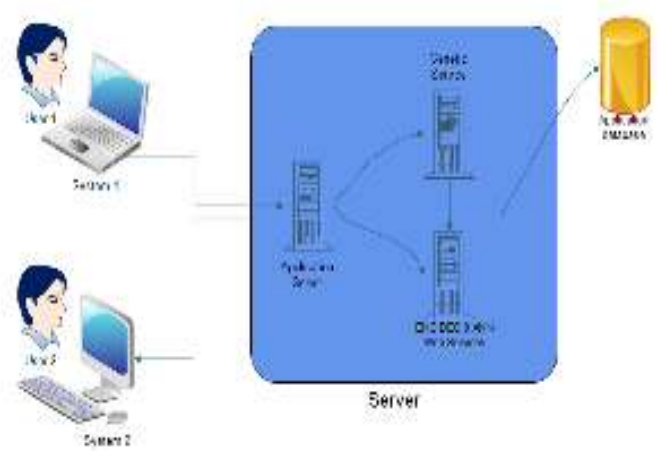

Fig. 2. System Architecture

After registration process if the user login`s for first time then at that time there is no history is present about his searches, but, as his login period & searches for any object increments the user`s history is maintained & next time the system will recommend some related topics to the recent searches.

In the normal procedure the user simply inputs search string & then the both distance algorithm& heuristic algorithm are applied over it. Finally, the paths which having shortest distance and which following match rule those are shown to the user.

IV. MODULES OF THE PROJECT

4.1 First Module: Genetic Algorithm

A genetic algorithm (or GA) is a search technique used in computing to find true or approximate solutions to optimization and search problem[2].

Steps for algorithm:

i. [Start] Generate random population of n chromosomes (suitable solutions for the problem)
ii. [Fitness] Evaluate the fitness f(x) of each chromosome x in the population
iii. [New population] Create a new population by repeating following steps until the new population is complete
    a. [Selection] Select two parent chromosomes from a population according to their fitness (the better fitness, the bigger chance to be selected)
    b. [Crossover] With a crossover probability cross over the parents to form a new offspring (children). If no crossover was performed, offspring is an exact copy of parents.
    c. [Mutation] With a mutation probability mutate new offspring at each locus (position in chromosome).
    d. [Accepting] Place new offspring in a new population
iv. [Replace] Use new generated population for a further run of algorithm
v. [Test] If the end condition is satisfied, stop, and return the best solution in current population
vi. [Loop] Go to step 2

4.2. Second Module: Neural Network Formation

In neural networks, learning is achieved mostly (but not exclusively) through changes in the strengths of the connections between neurons.

4.2.1 Mechanisms of learning include:

i. changes in neural parameters (threshold, time constants)
ii. creation of new synapses
iii. elimination of synapses
iv. changes in the synaptic weights or connection strengths

4.2.2 Hebbian learning rule

One common way to calculate changes in connection strengths in a neural network is the so called “hebbian learning rule”, in which a change in the strength of a connection is a function of the pre – and postsynaptic neural activities[1]. It is called the “hebbian learning rule” after D. Hebb (“When neuron A repeatedly participates in firing neuron B, the strength of the action of A onto B increases”.).If xj is the output of the presynaptic neuron, xi the output of the postsynaptic neuron, and wij the strength of the connection between them, and γ learning rate, the one form of a learning rule would be:

$$\Delta Wij\ (t) = \gamma * xj * xi \qquad (1)$$

A more general form of a hebbian learning rule would be:

$$\Delta Wij\ (t) = F\ (xj, xi, \gamma, t, \theta) \qquad (2)$$

in which time and learning thresholds can be taken into account.

4.2.3 Time

We often say that the connection strength increases when the pre- and postsynaptic neurons are active “simultaneously”. Simultaneous is very relative depending on the system under consideration! For example, when synaptic plasticity is induced in a brain slice preparation, simultaneous can be as short as several ms. However, when an animal learns an association between a food taste and sickness, simultaneous can be as long as several hours.

4.3. Third Module: Encryption

Data security and encryption are now a day's playing major role in Information Technology [IT] sector. Security problem generated creates exertion to the firm. They are several Digital Signature Algorithms which are useful in providing security for the issues generated. Elgamal Digital Signature [EDS][3] Algorithm which is used in wide applications had proved its efficiency in safe guarding the data .However due to different choppers the data is not firmly reaching the safe side. The previous methods proposed using this EDS Algorithm had given appropriate measures using several methods in protecting the data. But there are some flaws which made EDS Algorithm efficiency poor. In this paper, we are proposing an advanced EDS Algorithm with keys generated through statistical approach which consists of combination of random numbers and prime numbers blend with an Exclusive OR (⊕) operation to enhance the complexity for the key to be generated. We know that EDS Algorithm also ensures security and time complexity of improved signature. This proposed method can give us an authentication with a Digital Signature for decryption of the data at the receiver side very sanctuary.

4.4. Fourth Module: Decryption

Decryption is the process of converting the encrypted cipher text into plain text. Exactly reverse process.

4.4.1 Genetic Algorithm Module

In this research, the genetic algorithm module is used to find near-global optimal solutions for multiple objective functions. The procedure is described as follows:

Initialize operators and parameters of GA
While (Termination condition = FALSE) do
Begin
Population initialization
Selection
Crossover
Mutation
Replacement
End

Set chromosome structure and assign sub-goal weighting by the process parameter controller. Refine GA operators and parameters by the GA manager. The mathematical models for dynamic parameter setting In this research, we utilized a Genetic Algorithm approach, which can vary all of the process. Dynamic Parameter Setting is the methodology which is applied to find the optimal settings for the GA parameters. This function uses evolution evidence, which includes the population diversity and the level of the parents' fitness, to direct the dynamic settings of the GA parameters[2]. These models select the crossover and mutation rates based on the different problem type before the processing of each generation. The identification procedure contains three steps.

In the first step, the range value (Fr) of the population is divided into six regions, which are each assigned a range of the crossover and mutation rates for each generation. In the second step, if the members of parents and offspring are assigned to the first region, we assign the lowest crossover and mutation rate to preserve these best solutions. The highest crossover and mutation rate will be assigned to the worst members of parents and offspring which are ranked in the last region. The final step, calculates the actual crossover and mutation rates based on a transformation function varying of the member position in the population. Before the operations of crossover and mutation start, all members' fitness values will be identified and calculated as follows. The larger of the fitness values of the parents will be selected for the transformation function to determine the value of the crossover rate. The mutation rate is calculated by the position of the individual fitness value in the range. The situation factors (PFcn and PFmn) are the values, which are selected to tune the values of the crossover and mutation rates for specific problems.

4.4.2 Dynamic Parameter Setting of the Crossover & Mutation Rate

Rcn = (fmax - fl) / (fmax - fmin) pfcn Rmn = (fmax -fm) / (fmax - fmin) pfmn

where

Rcn = the range ratio for crossover operation from region 1 to region n.
Rmn = the range ratio for the mutation operation from region 1 to region n.
fmax = the maximum value in the population.
fmin = the minimum value in the population. L : the length of the solution.
fr = the range value between the maximum and minimum fitness value.
fl = the larger parent before the crossover operation.
fm = the larger parent before the mutation operation.
pfcn= the policy factor from region 1 to region n.
pfmn = the policy factor from region 1 to region n for the mutation operation.
h :a schema. fI :the fitness value. f :the average fitness value of the population.
f h :the average fitness value of schema h. l(h) :the defining length of schema h.
f h 2 :the average of the square of fitness values for the schema h.
Nh (t) :the number of solutions of generation t which are instances of the schema h.
nh (t +1)i :the expected number of offspring created in generation t+1 due to a solution i of schema h.

V. ADVANTAGES

1. Having no prior relation of next number from the previous ones**,** Great flexibility in relation to fast up and down scaling of resource needs.
2. Easier access to new versions.
3. GA approach is often applied for obtaining optimization and solutions in search problems.

V. DISADVANTAGES

1. Size of generated Pseudo random can be large at some conditions.
2. If we Give Incorrect input then the output of Rules generated will be wrong.

VI. APPLICATIONS

1. OTP and Data Management.
2. Security in Banking.
3. Security In Cloud
4. Can be used in knowledge Based Systems.
5. A PRNG is its own kind of cryptographic primitive, which has not so far been examined in the literature.
6. In particular, there doesn't seem to be any widespread understanding of the possible attacks on PRNGs, or of the limitations on the uses of different PRNG designs. A better understanding of these primitives will make it easier to design and use PRNGs securely.
7. A PRNG is a single point of failure for many real-world cryptosystems. An attack on the PRNG can make irrelevant the careful selection of good algorithms and protocols.
8. Many systems use badly-designed PRNGs, or use them in ways that make various attacks easier than they need be. We are aware of very little in the literature to help system designers choose and use these PRNGs wisely.

VII. CONCLUSION

In this paper, we propose an adaptive learning platform, where a security of data travelling on network will be more as an we are using artificial neural network with genetic algorithm for encryption of data using elgamal encryption algorithm so that every time when the user wants to send some information to the other user the encryption algorithm will generate a new key with the help of Artificial neural network and Genetic algorithm to generate random numbers. The keys generated will be unique and random in nature which will make the data more secure.

REFERENCES

[1] R. Mislovaty 1, E. Klein1, I. Kanter1, W. Kinzel2, "Security Of Neural Cryptography".

[2] Ragheb Toemeh1 and Subbanagounder Arumugam2," Applying Genetic Algorithms for Searching Key- Space of Polyalphabetic Substitution Ciphers".

[3] Ankita Agarwal IMSEC, Ghaziabad (India)," Secret Key Encryption Algorithm Using Genetic Algorithm"