ECC WITH SOFT COMPUTING: DESIGN OF A CRYPTOSYSTEM FOR DATA SECURITY IN E-LEARNING SYSTEM

P.K. Samanta[1], S. Karforma[2] and A. Bhowmik[*3]
[1]Department of Computer Science, The University of Burdwan, India
[2,3]Department of Computer Science, M.U.C. Women's College, India
*Corresponding Author: animca2008@gmail.com, anirbanbhowmik@mucwcburdwan.org

ABSTRACT

Now we are living in the era of ICT and over a period of time it is found that the education sector have changed its dimension from Guru-Shishya Parampara to class room teaching with the help of projectors or LED and now online teaching classes or teaching through E-Education portals or Web Based E-Education (WBEL) like Google classroom, Zoom, WebEx Meetings etc. Now the data security is the biggest issue in transferring any information or data through the Internet. E-education should comprise secure Internet technology for communication. Thus security issues should be added in the communication channel at any cost. In this paper, we have proposed an information security technique based on elliptic curve cryptography (ECC) and genetic algorithm to protect E-education system. A new digital signature mechanism (ECDSA)is introduced by integrating the concept of ECC, and integer theory that increases the robustness of our proposed technique compared to existing techniques. The performance of our scheme is analyzed through the security and privacy countermeasures against possible attacks. Different types of experimental results and statistical analysis prove the working efficiency of our proposed technique that utilized in E-education system.

Keywords: *ECC, Prime generator function, Genetic algorithm, Matrix operation, Digital signature.*

1. Introduction

The recent pandemic situation proves the utility of e-education in modern education system. At present e-education has changed the direction education sector in the world [24]. The three major criteria for e-education are

- Update, store, and exchange of information and its distribution;
- Internet technology helps to distribute the information to the end user.
- Targeting a wide field of education.

In any E-education system the core elements are the sharing of information, collaboration and interconnectivity via Internet. This system should be protected against fraudulent in order to maintain confidentiality, integrity and availability. Meanwhile, e-Education system demands a greater level of interoperability for applications and education environments in heterogeneous systems. The authenticated E-Education documents like education materials, certificates, and question papers, lecture materials, mark sheets which are communicated from user to user and in such a case the educational assets can be also modified or destructed [15].

Classification of Risks in E-Education

The e-education systems classified by goals of security computing integrity[33].

Table1: Threats in E-education system and computing

SL. No.	THREATS	SECURITY SERVICES
1	An unauthorized party gaining access of the education assets present.	Authentication and Confidentially.
2	An unauthorized party accessing and tempering with an asset used in E-education.	Integrity
3	Denial of service : Prevention of legitimate access rights by disrupting traffic during the Transaction between user	Availability and Confidentiality
4	Person's denial of participation in any transaction of documents.	Availability
5	Insecure cryptographic storage; insecure direct object reference; information leakage and improper error handling.	Availability, Confidentiality
6	Buffer overflow; cross site request forgery; cross site scripting; failure to restrict URL access; injection flaws; malicious file.	Integrity
7	Leakage of information by abusing communication channel.	Availability, Confidentiality, Integrity

In response to these threats, researchers have developed different types of solutions or countermeasures to improve security in E-education. At present e-education system become more user-centered and more secure with the help of new technologies such as robust cryptographic algorithm, digital right management, distributed firewall system, biometric authentication, digital watermarking etc.

Elliptic curve cryptography (ECC) was introduced in the mid-1980s by Koblitz and Miller [4] [14].It is a promising alternative process for cryptographic protocols based on the discrete logarithm problem in the multiplicative group of a finite field. ECC is one type of public key cryptosystem like RSA. ECC generates keys using the properties of the elliptic curve equation. An elliptic curve is a plane curve defined by anequation of the form $y^2 = x^3 + ax + b$ … (1), which is non-singular i.e., it has no self intersections or cusps. The curve is non-singular if the discriminant $4a^3 + 27b^2 \neq 0$, which is called the Weierstrass equation for an elliptic curve. The elements a, b, x and y are always belongs to R, Q, C or finite field F_q where $q = p^n$ with p prime and n≥ 1. If K is a field with $a, b \in k$, then the elliptic curve is said to be defined over K. The point (x, y) on theElliptic curve with $x, y \in k$ is called a K −rational point.The elliptic curve E:$y^2 = x^3 + ax + b$ over R has the following general form:

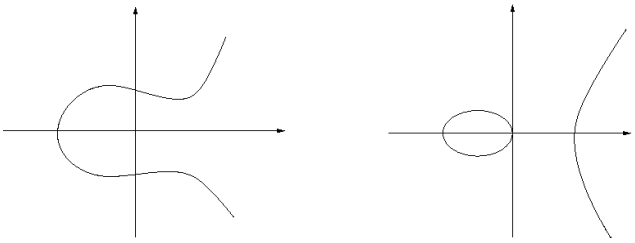


Fig1. Elliptic curve over R [12].

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field. Two families of elliptic curves are used in cryptographic applications: prime curves over Z_p and binary curves over $GF(2^m)$We know that a finite abelian group can be defined based on the set E_p(a, b) provided that $(x^3 + ax + b) mod\ p$ with condition $(4a^3 + 27b^2)\ mod\ p \neq 0\ mod\ p$. The rules for addition over $E_p(a, b)$, correspond to the algebraic technique described for elliptic curves defined over real numbers.

For all points $P, Q \in E_P(a, b)$:

1. $P + O = P$.
2. If P= (x_P, y_P), then P+ $(x_P, -y_P) = O$. The point $(x_P, -y_P)$ is the negative of P, denoted as –P.
3. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with P≠ $-Q$, then R= P+Q= (x_R, y_R) is determined by the following rules:

$x_R = (\lambda^2 - x_P - x_Q) mod\ p$ and $y_R = (\lambda(x_P - x_R) - y_P)\ mod\ p$where

$$\Lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P}\ mod\ p\ \ if\ P \neq Q \\ \left(\frac{3x^2{}_P - a}{2y_P}\right) mod\ p\ \ if\ P = Q \end{cases} \quad \ldots (1)$$

4. Multiplication is defined as repeated addition [5].

Generic Procedures for ECC: Here sender and receiver agree to some publicly-known data items which are (1) the elliptic curve equation (the values of a, b and the prime number p.). The elliptic group is computed from the elliptic curve equation and (2) a base point,B taken from the elliptic group. Each user generates their public and private key pair where private key = an integer,x selected from the interval $[1, p-1]$ and public key = product (Q) of private key and base point $(Q = x * B)$.

ECC provides the benefit like confidentiality, integrity, authentication and non-repudiation and it is used for its faster and efficient key generation process. It speeds up encryption, decryption and signature verification [13].

Genetic Algorithm: The genetic algorithm (GA) is a randomized search and optimization technique guided by the principle of natural genetic systems. At present GA is applied in various engineering fields. GA is a method of finding a good answer to a problem, based on feedback received from its repeated attempts at a solution. The objective or fitness function is a judge of the GA's attempts. The GA goes through the phases which are Evaluate, Select and Mateand Mutate until some kind of stopping criteria are reached. The GA performs a multidirectional search by maintaining a population of potential solutions. The

population undergoes a simulated evolution; at each generation the good solutions reproduce and bad solutions omit [16] [19].

2. Literature Survey

Ratha Paresh et. al.[1] has presented anencryption/decryption technique where the encryption key is generated from an arbitrary matrix. A set of operations between the generated key and original data block is performed for encryption and vice-versa in decryption. It is seen that the encryption process can be done by modifying the arbitrary matrix and multiple key can be generated for a single data block.

In this paper [2], a new security algorithm (combination of both symmetric and asymmetric key cryptographic techniques) is proposed for providing high security with minimized key maintenance. The three cryptographic primitives which are integrity, confidentiality and authentication are maintained here. Authors have combined the Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) to provide encryption and decryption. XOR-DUAL RSA algorithm is used for authentication checking and Message Digest-5 (MD5) for maintaining integrity.

Rani Sheeba S.et. al. [3] have discussed about a low-cost Public Key Cryptography (PKC) based security approach for authentication, digital signature etc. It is a software approach using Elliptic Curve Cryptography (ECC) over GF ($2m$) in order to obtain stronger cryptography using Koblitz curves and TNAF (τ- adic non-adjacent form) with partial reduction modulo. Authors have examined the mathematical concept behind the group of torsion points. Authors have discussed about the definition and implementation of discrete logarithm problem using $E(Fq)$ and also showing how this technique can be used in both encryption and key exchange protocols.

Das A. K. et. al. [6]have described about the key things in any secure communication between any two neighboring sensing devices on the Internet of Things (IoT) environment. The key elements are secure device access control in secure way (node authentication) and key agreement protocol between devices. Here the node authentication is done by using their pre-loaded secret credentials in memory. In this paper, authors have proposed a new certificate-based lightweight access control and key agreement protocol in the IoT environment that utilizes the elliptic curve cryptography (ECC) along with the collision-resistant one-way cryptographic hash function.

In [9] the author has outlined a structure which is basically identical to an LFSR except for the delay elements being replaced by inverters. The feedback positions are labeled by switch values f_i. If f_i=1 then the switch is closed and otherwise it is open. The switch values can be represented more conveniently in terms of the feedback polynomial which is given as follows.

$$f(x) = \sum_{i=0}^{r} f_i x^i \text{Where } f_0 = f_r = 1.$$

It is important that the oscillator is not stuck in a single fixed rate. The FIGARO (**Fi**bonacci-**Ga**lois-**R**ing-**O**scillator) TRNG design simply XORs the output of a FIGARO oscillator with the output of a Galois oscillator and samples the XOR output. The author also introduces a self-controlled LFSR for post-processing of the output.

In[10] a PUF based key agreement scheme is described for Internet of Things (IoT) which is not vulnerable for man-in-the-middle, impersonation, and replay attacks. This scheme also offers identity based authentication and repudiation based onthe concept of elliptic curve multiplications and additions.

Momeen Khan et al [36] focused on security concerns and its solutions that can make the education management system secure from any possible potential threats and attacks.They have proposed a complete multi-layered security model that will provide a very secure environment for any education management system.

3. Our Contributions

Section 1and Section 2 of our article has discussed about significance of e-education, its threats and different types of cryptosystem, techniques, and methods for improving security in E-education system. Despite the use of different types of cryptographic tools in these techniques, there are still some loopholes exists. Here we have emphasized on the development of cryptosystem but utilizing the benefits of ECC with soft computing for

securing e-education system. The key features of our scheme are given below:

a. Information security based on elliptic curve cryptography and soft computing used in E-Education system.
b. Elliptic curve generation using prime number generator functions like Euler, Legendre, Honaker etc.
c. Application of ECC, GA operators (two points cross over operator) and fitness function in key generation.
d. Digital signature based on ECC and modulo operation.
e. A new encryption model based on matrix operations.

4. Flow Chart of Proposed Technique

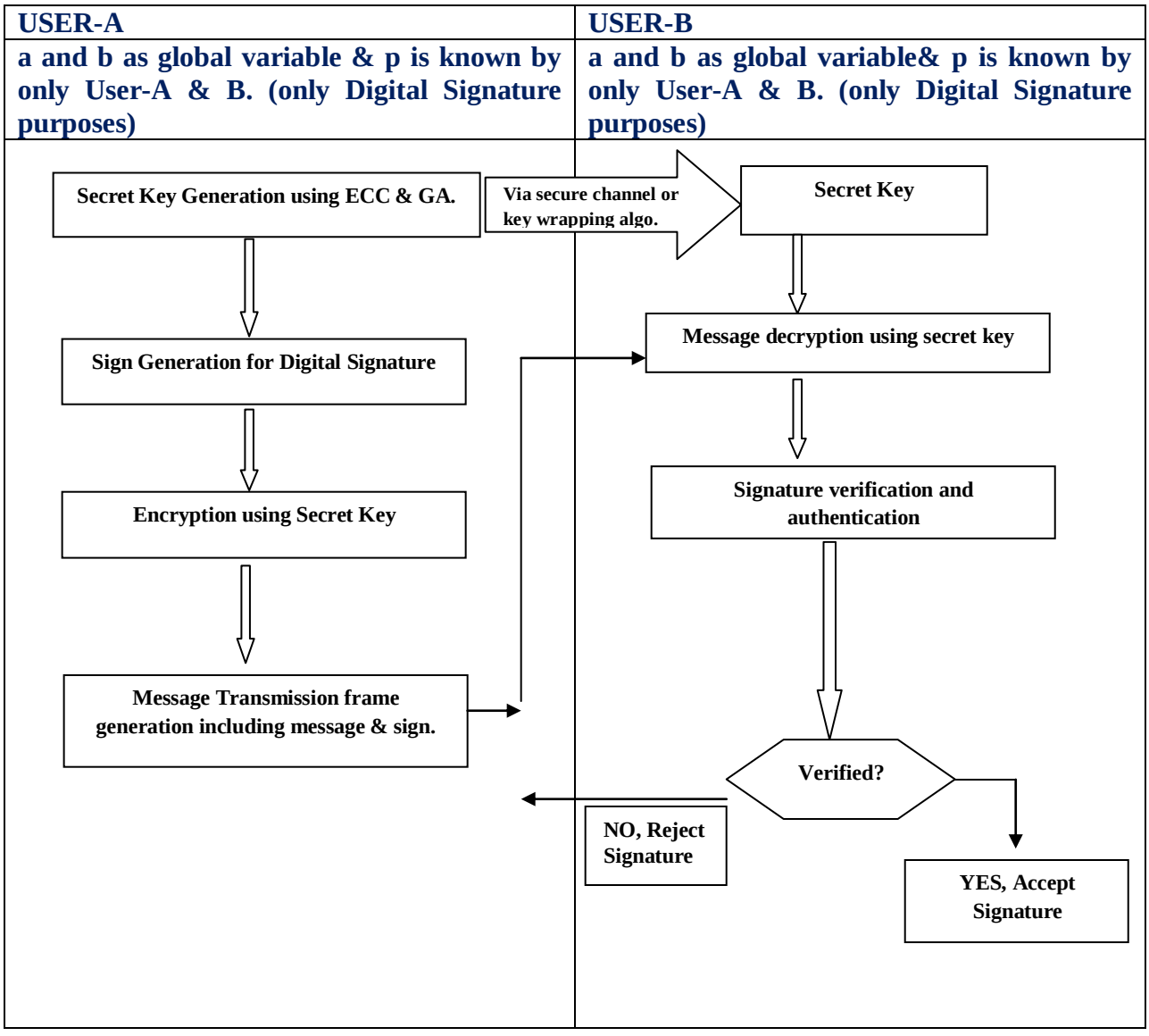


Fig2: Flow diagram of proposed technique

5. Proposed Methodology

Our proposed technique is divided into three modules. Each module is described through proper algorithms.The details are given below.

5.1 Module-1

*Theory:*This module focuses on secret key generation based on ECC and genetic algorithm. Here we have emphasized on elliptic curve overZ_p. For prime curve overZ_p,

we have used a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through $p-1$ and the calculation are performed on modulo$p$ .For elliptic curve over Z_p, we have limited ourselves to equations of the form
$y^2 = x^3 + ax + b$, but in this case with co-efficient and variables limited to Z_p.

$$y^2 mod p = (x^3 + ax + b) mod p \ldots (1)$$

Now we have considered the set $E_p(a,b)$ consisting of all pairs of integers (x,y) that satisfy equation (1), together with a point at infinity O. The coefficients a and b and the variables x and y are all elements of Z_p with the condition $4a^3 + 27b^2 \neq 0$ .Here we have used two random values and a prime number in elliptic curve generationonZ_p.

We have taken n (2,4,8, ...) number of points from equation (1) to generate a key of size $4k$. Genetic two points cross over operator along with afitness function (objective function) is used for getting better result in key generation.
This secret key is transmitted to recipient end through secure channel or via any key wrapping algorithm. This secret key used for encryption in e-education system.

Algorithm-1: (Secret Key Generation)

Mathematical Tools:(1) Two prime generator functions such as $fn\_prm_1(\,)$ and $fn\_prm_2(\,)$ with two Parameters,
(2) Genetic operator (Two point crossover operator)
(3) Two linear function such as
$fn\_ln1(\quad)$, $fn\_ln2(\quad)$.
(4) Addition and Multiplicationw.r.t. elliptic curve.
(5) Fitness function.
*Input:*Two real numbers.
*Output:*Secret key of size $4k$.
Methods:
Step1:Set a, b, m, pr , r_1, r_2 as integers and $poln\,[\,][\,], Enc\_key\,[\,], Child\_key\,[\,]$ as array.
Step2: $a\leftarrow$ real number$_1$ and $b\leftarrow$ real number$_2$.
Step3: $for\ i = 0\ to\ p$ {/***p is the number of population and even number****/}
Step4: $r_1 \leftarrow fn\_ln1(a,b)$ and $r_2 \leftarrow fn\_ln2(a,b)$.
Step5 : $k_1 \leftarrow fn\_prm_1(r_1, r_2)$, $k_2 \leftarrow fn\_prm_2(r_1, r_2)$ and $k_3 \leftarrow fn\_prm_3(r_1, r_2)$.

{/* $fn\_prm_3()$ is generatedby adding 1 with the coefficients of the polynomial of $fn\_prm_2()$.*/}
Step6: Arrange k_1, k_2, k_3 in ascending order and $a \leftarrow k_1$, $b \leftarrow k_2$ and$pr \leftarrow k_3$.
Step7: Generate points on the elliptic curve$E_{pr}(a,b)$.
Step8: Take n number of different points from $E_{pr}(a,b)$such that for any point (x_i, y_i),$x_i \neq 0$, $y_i \neq 0$.
Step9: Arrange these n points in ascending order on basis of values ofx_i. Thus we have got an array of
$m$elements from these n points where $m = 4k$.
Step10: $poln[i]\,[m] \leftarrow m$elements from step8.
end for.
Now we have applied GA on $poln[\,][\,]$ to generate encryption key. Here we have used two point cross over GA operator with afitness function (objective function) on the population ($poln\,[\,][\,]$) to generate best solution.The function two_PtCrossOver ( ) is used for two point cross over on genetic materials. Here two arrays are used as genetic materials (parent chromosomes) for two point cross over in the said function.In each time the two_PtCrossOver ( )produces two arrays as child chromosomes. The fitness function (objective function) is used for getting bestkey stream from child chromosomes based on specific condition.
Step11: for $j = 1\ to\ p$
Step12: $Child\_key1\,[\,] \leftarrow$ Call *two_PtCrossOver*($poln[j][m], poln[j+1][m])\ and\ Child\_key2\,[\,] \leftarrow$ Call *two_PtCrossOver*($poln[j][m], poln[j+1][m]$)
{/* according to value of fitness function Child_key1 [ ] or Child_key2 [] is used as encryption key.*/}
Step13:
$Enc\_key\,[\,] \leftarrow$
$call\ fitns\_fnc(Child\_key1[\,])orcall\ fitns\_fnc(Child\_k$
$j = j + 2$
End for
Step14: End.
The Enc_key [ ]is the required secret key for encryption-decryption purposes.

5.2 Module-2

Theory: This module focuses on a new digital signature scheme based on ECC and hash

function. Message authentication protects two parties who exchange messages from any 3rd party. But it does not protect the two parties against each other. In this situation where there is not complete trust between sender and receiver, something more than authentication is needed. The digital signature is the most popular solution to this problem.The digital signature has the following properties:

1. It must verify the author and the date and time of the signature.
2. It must authenticate the content at the time of the signature.
3. It must be verifiable by the 3rd party, to solve the disputes.

Thus the digital signature function includes the authentication function.

Digital Signature Requirements:

a. The signature must be bit pattern that depends on the message being signed.
b. The signature must use some information unique to the sender to prevent both forgery and denial.
c. It must be relatively easy to produce the digital signature and also easy to verify.
d. It must be computationally infeasible to forge a digital signature.

Elliptic curve digital signature algorithm (ECDSA) is enjoying increasing acceptance due to the efficiency advantage of ECC, which yields security comparable to that of other schemes with a smaller key bit length.

Here user-A and user-B both generate same ECC structure at the same time based on global parameters and prime number. So no data transmission is required before signature generation.After signature generation only verification data is transmitted with cipher text.

Algorithm-2:(Digital Signature Generation and Authentication)

Mathematical Tools:

1. Prime number generator function.
2. XOR and modulo operation.

*Input:*Two real numbers which are treated as global domain parameters.

Output: Signature verification.

Methods:

The two real numbers a &b are sent from user-A to user-B via public channel. Using prime generator function the prime number p is generated and the required ECC is created in both sides.

	USER-A	USER-B
Step-1	a, b & pWhere a & b are open to all but p is not open to all.	a, b & pWhere a & b are open to all but p is not open to all.
Step-2	Select a point$u$ in ECC and send to the user-B through public channel.	Select a point$v$ in ECC and send to the user-B through public channel.
Step-3	Calculate $k_1 = orderOf\ (\ u\ )$ & $k_2 = orderOf\ (v)$	Calculate $k_1 = orderOf\ (u)$ &$k_2 = orderOf\ (v)$
Step-4	Now (p+1) is even number and can be expressed in the form (2^a m) with m odd i.e., 2^a is the largest power of 2 that divides (p+1).	Now (p+1) is even number and can be expressed in the form (2^am) with m odd i.e., 2^a is the largest power of 2 that divides (p+1).
Step-5	Calculate $G = (u + v) * m$	Calculate $G = (u + v) * m$
Step-6	Let G=(X,Y) and $r = X\ mod\ a$	Let G=(X,Y) and $r = X\ mod\ a$
Step-7	$e = Hash(msg)$Where msg is the message to be send.	
Step-8	S=(e $\oplus$ r) mod $(k_1 + k_2)$	
Step-9	Create a format Encrypted message | S This is sent to the user-B where S is used as signature part.	Decrypt the message using secret key and calculate $e = Hash\ (msg)$
Step-10		Calculate $S' = (e \oplus r)\ mod\ (k_1 + k_2)$
Step-11		Compare S and S' and verify.

In e-education system User-A and User-B may be students, teachers, academic official staffs etc.

5.3 Module-3

Theory:This module has described about a novel encryption and decryption model based

on Matrix operations. Here we have used a matrix function that takes secret key and block of plain text as input and producesblock of cipher text. The whole plaintext is divided into n numbers of block. The size of each block is equal to the size of secret key.The key size is $4k$. If there is some remaining bytes exist for plain text then it may be 1 to (key size-1) bytes. So operations in this last block are not same as that of the previous blocks.The details descriptions are given below.

Algorithm-3: (Encryption & decryption)

Mathematical Tools:

a. XOR operations.

b. Matrix Elementary Transformations: Interchange any two rows and columns of matrix.

c. The following algorithm is only for one block. If there are n number of blocks of plain text then this algorithm should apply n times.

*Input:*Multiple block/blocks of Plain text.

Output: cipher text.

Methods:

Step1: Let skey [r] [4], plt [r] [4], res1 [r] [4],res2 [p], rmn_plt [p], cipherT,len as integer.

Step2: exky[4]={(skey[1][1]+1)H, (skey[1][2]+2)H, (skey[1][3]+3)H, (skey[1][4]+4)H}{**/*H for Hex number*/**}

Step3: call $matrix\_function(\ skey, plt)$.

Step4: end.

Procedure:

$matrix\_function(\ secret\ key, plaintext)$

Step1: for i=1 to r {**/* r is the number of rows of secret key*/}

for j=1 to 4

res1 [i] [j] = skey[i] [j] ⊕ plt[i] [j]

end for

end for

Step2: for i=1 to r

for j=1 to 4

res1 [i] [j] = exky[i]⊕ res1 [j] [i]

end for

end for

{/* elementary operation on resultant matrix for cipher text generation*/}

Step3: res1[r] [4] ← ($R_1 \longleftrightarrow R_2$) res1 [r] [4] and res1 [r] [4] ← (C_3 C_4) res1 [r] [4]

{/* encryption of remaining part of the plain text /*}

Step4: Set len ← get_length (rmn_plt[ ]) {*/ rmn[p] represents remaining part of the plain text*/}

Step5: tmp_key [len] ← call extract_Key (skey[r] [4], len) {*/ first *len* number of values are extracted from s key [r][4] which is equal to length of remaining plain text*/}

j←0

for i=1 to len

res2 [i] = tmp_key[i] ⊕rmn_plt [i] ⊕exky [j++]

if (j==4) then j←0

end for

Step6: cipherT = res1 [][] + res2 [].

Step7: End.

So cipherT is the required cipher text which is generated from plain text. This cipher text is transmitted to the receiver end through wireless channel. A frame format is used for ciphered message transmission which is discussed in algorithm-2, step-9. The format is given below.

Ciphered message	S

S is taken from module2 which is used for signature verification purposes.

*Decryption:*The decryption process is just the reverse of encryption process. The details of the process are given below.

Algorithm 3.1 (Decryption Process)

Input: secret key, ciphertext.

Output: Plaintext.

Method:

Step1: Separate the n number of blocks and remaining parts.

Step2: Xor operation is done between exky [] and blocks and remaining parts of cipher text.

Step3: Matrix elementary operation ($R_1 \leftrightarrow R_2$) and ($C_3 \leftrightarrow C_4$) is done on resultant matrix (i.e., block) of Step2.

Step4: Xoroperation between secret key and resultant matrix (i.e., block) of step3.

Step5: Plain text generation.

Step6: end.

6. Experimental Results& Discussions

In this section, we have performed several experiments and tests to evaluate the security and robustness of our proposed technique.We have performed all the experiments using Cryptool interface.

6.1 Statistical Tests & Randomness Tests:

A. Autocorrelation Analysis:

Autocorrelation or serial correlation tests [20] [22] [23] describe the correlation amongst numbers and compares with the pattern correlation to the expected correlation of zero. The evaluation of autocorrelation is used for locating repeating styles. In statistics, the Autocorrelation or serial correlation of a random manner is the Pearson correlation among values of the system at different instances. The mathematical formulation for Pearson correlation system is given beneath.

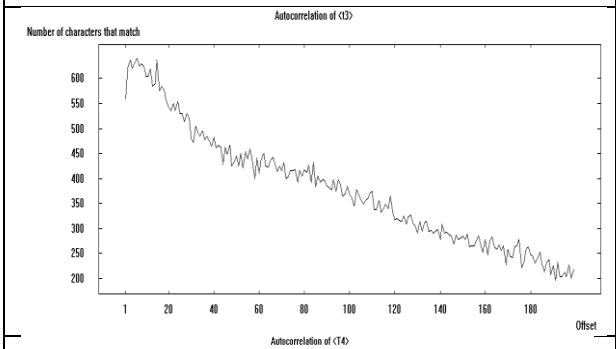
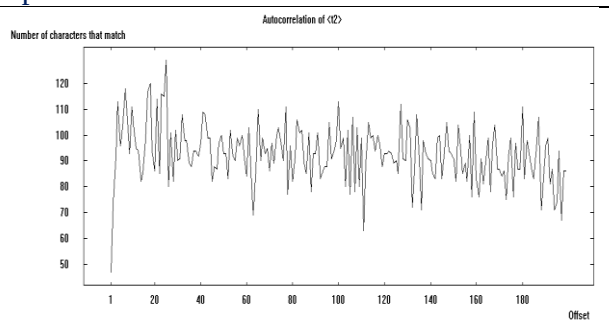
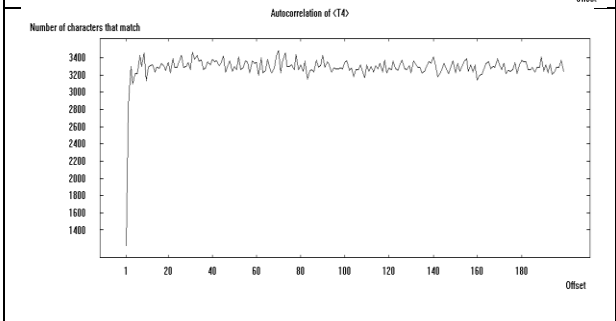
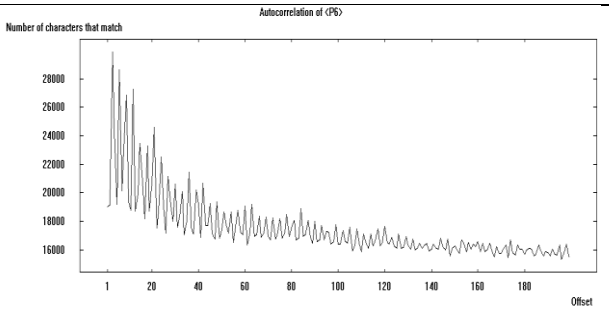
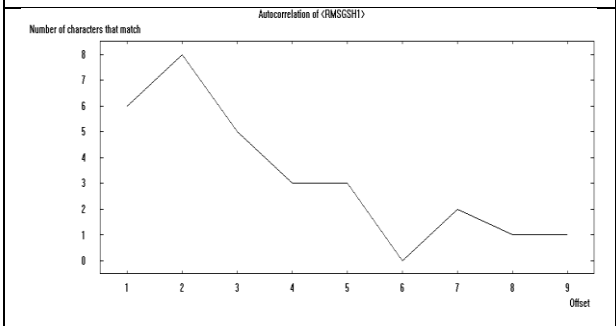
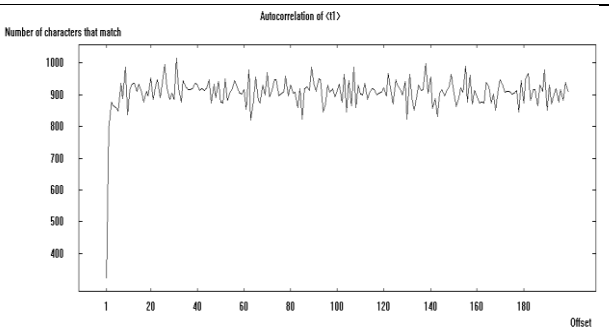
$$r = \frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{N}(y_i-\bar{y})^2}} \quad \ldots (1)$$

For autocorrelation, this coefficient is computed between the time collection and the identical time series lagged

by means of detailed range of periods. Here only graphical representation is given for our technique. The

following figures show the autocorrelation between plain texts and cipher texts with same key.

Secret Key: - ***Ab@9732381***

Plain Texts	Cipher Texts
	
	
	

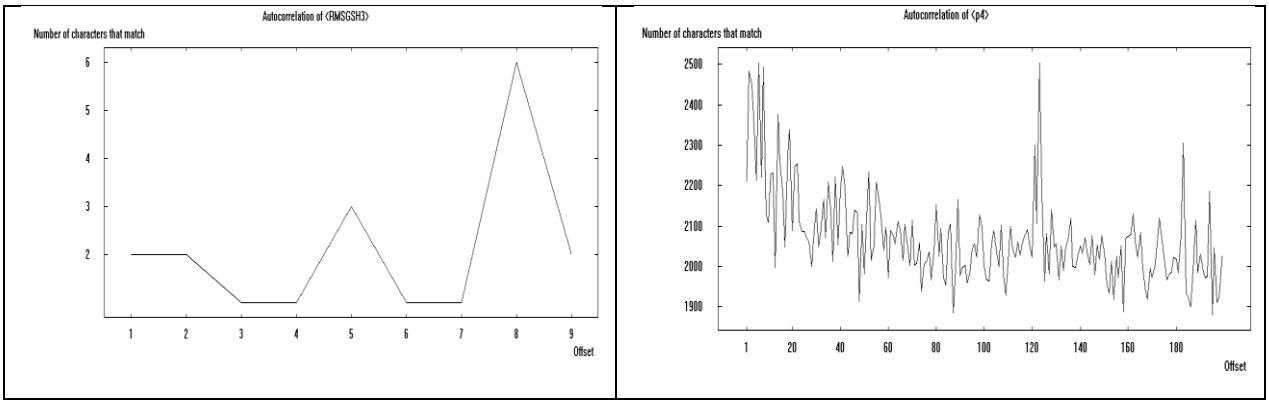


Fig3: Autocorrelation analysis of proposed scheme

B. Serial Test for Randomness:

The serial take a look at [17][21][30] and chi-rectangular check[29] are comparable on frequency. The distinction is that the chi-square relative frequency take a look at examines whether or not or no longer man or woman values are consistent with a uniform distribution and the serial take a look at examines whether or not sequential and non-overlapping pairs of random numbers have a uniform distribution. This test focuses on frequency distribution of pairs of samples. The random numbers are grouped right into a quite small quantity of businesses by using the usage of serial check. The random numbers from the generator are mapped right into a quite small amount of remarkable integer values from 10 to 181 by means of way of the modulo feature [31]. With those numbers of distinct values, the huge style of agencies additionally is affordable, from one hundred to 32,761. A chi-square cost checks different pairs are similarly possibly values. The mathematical formulation is given below.

$$T_2 = \frac{4}{M-1}((M00)^2+(M01)^2+(M10)^2+(M11)^2) - \frac{2}{M}((M0)^2+(M1)^2) + 1 \ldots (2)$$

Where $M00:$ number of $00's$ in the key stream. $M11:$ Number of $11's$ in the key stream. $M01$: Number of $01's$ in the key stream. $M10$: Number of $10's$ in the key stream. M: Total size of key stream. The following table2 and figure4 shows the randomness of generated key by our cryptosystem.

Table2:Serial test data of our scheme

Key size (bits)	Serial test of our scheme	Test on key by PRNG	Test on key by TRNG	Test on key by FIGARO
56	4.0016	4.0636	4.1352	3.9831
64	4.1120	4.0973	4.1872	4.1092
128	4.1765	4.1643	4.2021	4.2043
192	4.2147	4.1892	4.4454	4.1998
256	5.0103	5.0183	5.0090	4.2102
328	5.1971	5.2201	5.1066	4.2206
416	5.6782	5.5705	5.1331	4.2564
1024	8.0098	8.1010	5.3050	4.3020

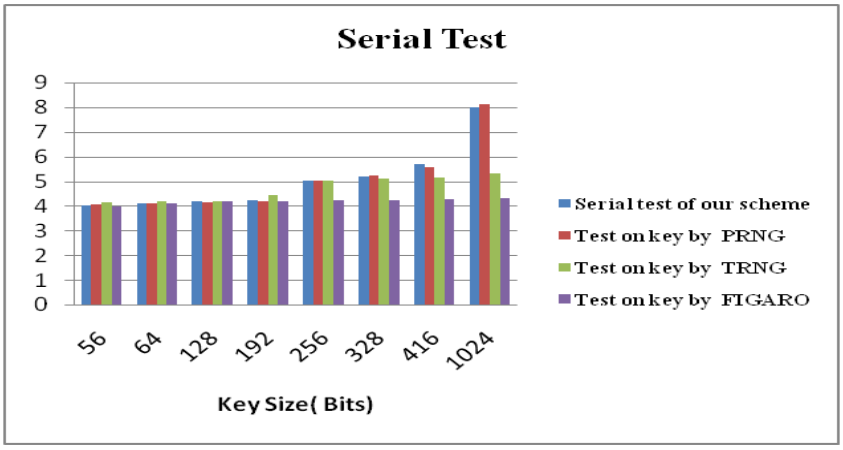


Fig4: Graphical representation of table1.

C. Information Entropy:

Entropy measures have gained widespread use in the analysis of complex real-world data. The term "entropy" first originated in the field of thermodynamics and can be interpreted as the amount of information needed to completely specify the physical state of a system. A very orderly and regular system has a low entropy value.

A high entropy score indicates a random or chaotic series, whereas a low score indicates a high degree of regularity.

Entropy measures:

Sample Entropy (m, r) : SampEn is calculated based on the negative natural logarithm of the conditional probability with m length dataset. It is given that it has repeated itself for m points (within a tolerance limit r that is commonly based on the standard deviation of the data) and also for (m+1) points. SampEn can be calculated using the following formula: $SampEn = -\log\frac{A}{B}$, where A is the number of pairs of vector subsets of length m+1 which has a distance function less than r, while B is the number of pairs of vector subsets of length m which similarly has a distance functions less than r [26] [32].

Permutation Entropy (n): It is used to check the presence of noise in real world data. For a time series $\{x_1, x_2, \ldots, x_{N-1}\}$ this entropy algorithm splits the data into overlapping n-tuples, where n is the embedding dimension. Each n-tuple is then sorted in ascending order. Now this sorted tuple generates π (permutation type) according to the ordering of the sorted data. There will be n! Possible permutation types according to embedding dimension n. The relative frequency p (π_i) is determined for eachπ_i, for $1 \le i \le n!$, according to the following equation [33]:

$$p(\pi_i) = \frac{number\,of\,occurrences\,of\,type\,\pi_i}{N - n + 1}.$$

The permutation $H(n)$ is then calculated as follows:

$$H(n) = -\sum_i^{n!} p(\pi_i) \log p(\pi_i).$$

Where $0 \le H(n) \le \log(n!)$. Here 0 indicates a series that is Monotonically increasing or decreasing and log n! Indicates a completely random series. When experiment

Occur, $H(n)$ is rescaled by dividing by log n! thus normalizing $H(n)$ to return values between 0 and 1 with 0

Indicating highly regular data and 1 indicating maximal entropy[27].

Permutation Test (t):The permutation test is done for test of randomness. It is performed by first partitioning the original timeSeries into groups of t elements. When the original time series is not perfectly divisible by t , the remaining data points are discarded. The ordering of the element indices are obtained from the sorted elements of each group. In each group the possible orderings is $t!$ Now the chi-square test can then be performed with t! categories and the probability of each distinct ordering is $1/t!$ The chi-square statistic is interpreted as the distance from the expected value given by the null hypothesis and the uniformly

distributed input data. Thus a high value indicates a high degree of regularity and a low value indicates a high likelihood of the null hypothesis being true[28].

The main difference between permutation test and permutation entropy is that the partitions in the permutation test do not overlap, and the permutation entropy algorithm calculates H (n).

Table3 (a): comparative data analysis on Uniform (0, 1) series

	T.val 1	T.val -2	T.val 3	T.val 4	T.val 5	T.val 6	T.val 7	T.val 8	T.val 9	T.val 10
Sample Entropy	0.73	0.41	0.50	0.56	0.95	0.61	0.48	0.84	1.14	0.64
Permutation Entropy	1.20	0.40	0.72	0.58	1.0	0.88	0.60	0.54	0.69	0.51
p test	0.52	0.98	0.63	0.73	0.82	0.42	0.77	0.59	0.64	0.97

Table3 (b): comparative data analysis on Gaussian (0, 1) series

	T.val 1	T.val 2	T.val 3	T.val 4	T.val 5	T.val 6	T.val 7	T.val 8	T.val 9	T.val 10
Sample Entropy	0.43	0.41	0.59	0.56	1.3	0.61	0.41	0.74	1.1	0.65
Permutation Entropy	1.00	0.92	0.73	0.63	0.41	0.83	0.62	0.52	0.89	0.44
p test	0.61	0.78	0.83	0.45	0.54	0.44	0.93	0.61	0.64	0.71

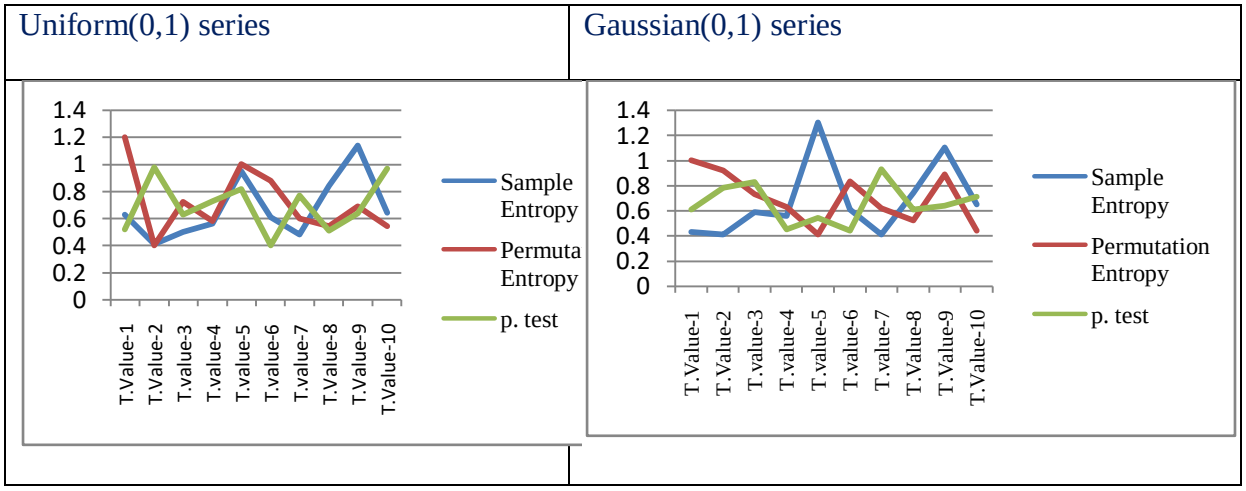


Fig5 (a): Graphical representation of table 6(a)

Fig5 (b): Graphical representation of table 6(b)

Observations: Tables 3 (a), 3 (b) & Figures 5(a), (b) above show the comparative data analysis and resulting scores of Sample entropy, Permutation entropy and the permutation test chi-square statistic. For better comparison, all scores for the various metrics are rescaled in between 0 and 1.4. In addition, the inverse of the natural log is applied to the chi-square statistic from the permutation test. This was done to invert the plots to better correspond with the interpretation of the entropy measures, i.e. a high value corresponds to low regularity and a low value correspond to high regularity.

D. Key Sensitivity & Avalanche Effect:

An ideal encryption technique should be sensitive with respect to the secret key i.e. a single bit change in the secret key should produce a completely different cipher text. For testing the degree of key sensitivity of the proposed encryption procedure, we have performed the encryption process in the files (.txt, .docx, .pdf etc) with slight changes in the secret key. The avalanche effect is shown below only for changed secret key. The following table4 and graph (Fig.6) shows the total scenario of avalanche effect of our proposed scheme [35].

Table4: Avalanche effect on secret key

Key	Total number of added characters	Total number of deleted characters	Total number of changed characters
Ab@9732381 (Original key)	2526	1545	2543
Eb@97**4**238**2**	3216	3010	2262
A**B**@97323**&0**	3724	2938	2371
A**n#**9732387	3908	3376	2287
ab@**3**73**3**381	3619	3630	2418
A**B%**97**X**2381	4162	4145	1492
Ab@9***()**381	3595	3748	2104
Mb@87**4**2381	3878	3825	2215
AbC973271	4125	4051	2129
Sc$9732381	4001	4098	2062

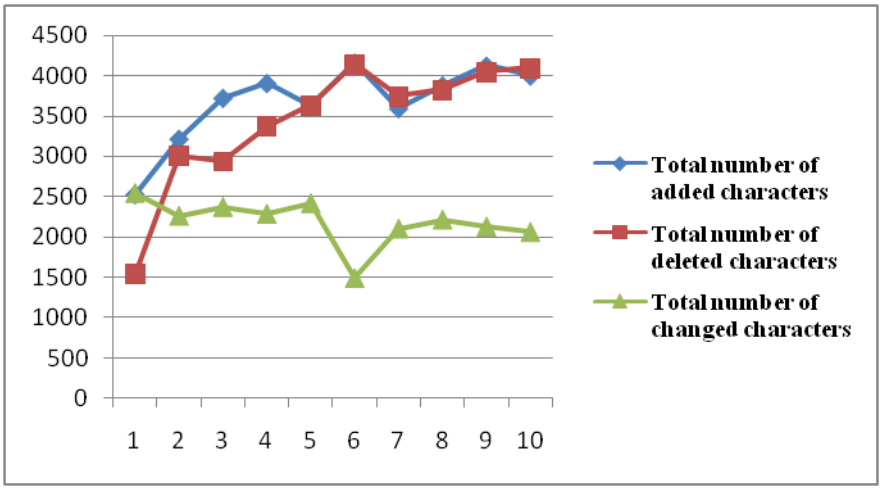


Fig6: Graphical analysis on table3.

6.2 Attacks Analysis:

Brute Force Attack:

A brute force attack (or exhaustive search) is a cryptographic hacking that uses trial-and-error method to guess possible combinations for secret keys used for logins, encryption keys, or hidden web pages[18]. We can defend against the brute force attack in the following ways:

a) Increase key length
b) Increase key complexity
c) Limit login attempts
d) Use multifactor authentication.

In this article we have used secret key for encryption and decryption and we have focused on key length and key complexity. In our scheme a complex key generation process is used to generate secret key. It is also seen that brute force attack is infeasible in case of large key space. In this attack, attacker uses every possible keys to translate the cipher text into plain text. On average, half of all possible keys are enough for deciphering the text. Here algorithms are known to all but if it uses large key space then brute-force attack will impossible. An example is given below.

At present the fastest super computer is Fugaku (Japan)with HPC technology having speeded 415.5 peta FLOPS i.e., 415.5X 10^{15} floating point operations per second. Let us consider each trial requires 3000 FLOPS to complete one check. So number of trials complete per second is: $138.05x10^{12}$. The number of second in a year is: $365 * 24 * 60 * 60 = 3153600\ sec$.Now from the above key space the formula for break the key is $2^k / (138.05 * 10^{12} * 3153600) = Y, Y$ denotes number of years. So if k increases then Y increases ($k \infty Y$) thus for large key length it is difficult to break the key. A cipher text with such a long key space is sufficient for reliable practical use. This proves that a key with longer length is sufficient enough to overcome the brute force attack.

Confidentiality Attack:

This attack tries to expose or disclose the confidential data to unauthorized persons. This may be transfer of e-contentsto the unauthorized persons and as a result hacker can modify e- contents. Example includes: Group session eavesdropping, Group identity disclosure [34]. Strong encryption and authentication protocol should to be used to counter confidentiality attack.

6.3 Performance Analysis & Comparison:

In this section we have discussed about the performance metrics of our scheme w.r.t security strength of encryption key.

Encryption Key Security Strength: -In this section we have discussed about the security strength metric of encryption key. It is an important metric to analyze the proposed key generation method. Here we have proposed architecture of soft computing based key generation to provide high security to sensed data and to protect data against malicious users. The security strength metric is measured with respect to key size [25].

The security strength metric is evaluated to measure the security level of the proposed key generation technique in any platform like telehealth sector, cloud computing, big data, data warehouse etc. The proposed security method achieves better security strength than the existing hardware based methods and software based methods. This superiority of the proposed method can be attributed to the proposed highly secure encryption key generation technique for sensed data. Figure 7&8 depicts the comparison of security with different hardware based and software based security schemes for sensitive data encryption and transmission. Hence, the proposed key generation technique achieves maximum security strength than other existing scheme.

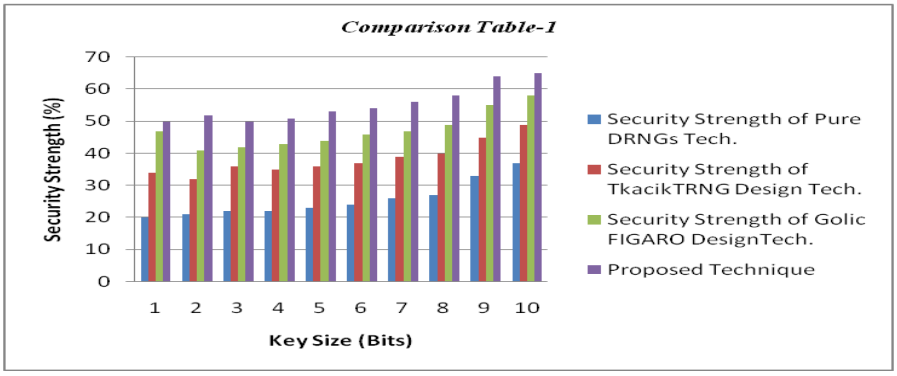


Fig7. Comparison among hardware based technique & proposed technique

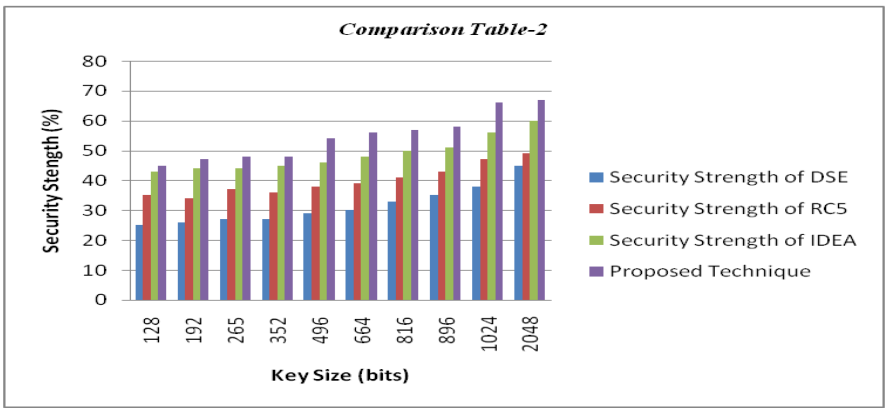


Fig8. Comparison among software based technique& proposed technique

Comparison among different techniques:Here we have described a comparative study among different techniques through the following table5.

Table5: Comparison w. r.t. different attributes among different techniques.

Attributes	**Ref. [6]**	**Ref. [7]**	**Ref. [8]**	**Ref. [10]**	**Ref. [11]**	**Ref. [31]**	**Ref. [32]**	**Ref. [36]**	**Proposed Technique**
Confidentiality	Yes	No	Yes	No	Yes	Yes	Yes	No	Yes
Integrity	No	No	Yes	No	No	Yes	No	No	yes
Authenticity	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes
Defend against Man-in – middle attack	No	No	Yes	Yes	No	No	Yes	No	Yes
Defend against replay attack	Yes	Yes	No	Yes	No	No	No	Yes	Yes
Cryptanalysis	No	No	Yes	No	Yes	Yes	No	Yes	Yes
Session key establishment	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes
Privacy Protection	Yes	No	Yes	No	Yes	No	Yes	Yes	Yes
Vulnerability	No	No	Yes	No	Yes	No	Yes	No	Yes

7. Conclusions

The E-education system has taken an important role in the modern teaching and education process. In pandemic situation this system is massively used among universities, colleges, and schools for different academic purposes and as a result security problems have come as vital issue. In this paper, we have presented architecture of cryptosystem for giving security in e-education system. Our cryptosystem is based on ECC and genetic algorithm with minimal computational overhead. A new digital signature protocol is introduced using integer theory, and ECC. We have introduced the concept of elementary matrix transformation in case of data encryption and decryption. Different types of statistical analysis, attack analysis, performance test and comparative analysis are done to prove the efficacy of our proposed cryptosystem in e-education system.

References

1. Ratha, Paresh, Debabala Swain, Bijay Paikaray, and Subhadra Sahoo. "An optimized encryption technique using an arbitrary matrix with probabilistic encryption." Procedia Computer Science 57 (2015): 1235-1241.
2. Rawya Rizk, Yasmin Alkady,Two-phase hybrid cryptography algorithm for wireless sensor networks, Journal of Electrical Systems and Information Technology, Volume 2, Issue 3, 2015, Pages 296-313, ISSN2314-7172, https://doi.org/10.1016/j.jesit.2015.11.005.
3. S.Sheeba Rani et al., 2017, Performance analysis of conventional pitch angle controllers for DFIG" in International Journal of pure and applied mathematics, Vol. / Issue / Page No: 1-9 Vol 116 No. 12 October 2017.
4. Ankur Lohachab, Karambir, ECC based inter-device authentication and authorization scheme using MQTT for IoT networks, Journal of Information Security and Applications, Volume 46, 2019, Pages 1-12, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2019.02.005.
5. Kumar, M., Chand, S. ESKI-IBE: Efficient and secure key issuing identity-based encryption with cloud privacy centers. Multimed Tools Appl 78, 19753–19786(2019). https://doi.org/10.1007/s11042-019-7155-x.
6. A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodriguez and Y. Park, "Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment," in IEEE Access, vol. 7, pp. 55382-55397, 2019, doi: 10.1109/ACCESS.2019.2912998.
7. Ostad-Sharif, A., Abbasinezhad-Mood, D. & Nikooghadam, M. A Robust and Efficient ECC-based Mutual

Authentication and Session Key Generation Scheme for Healthcare Applications. J Med Syst 43, 10 (2019). https://doi.org/10.1007/s10916-018-1120-5.

8. M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020, doi: 10.1109/ACCESS.2020.2980739.
9. J. Dj. Golic, New methods for digital generation and post processing of random data. IEEE Transactions on Computers 55(10): 1217—1229, 2006.
10. Braeken, A. PUF Based Authentication Protocol for IoT. Symmetry 2018, 10, 352. https://doi.org/10.3390/sym10080352.
11. W. Stallings, Cryptography and Network Security: Principles and Practice, third edition, Prentice Hall, 2003.
12. Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill publishing company, New Delhi, 2008
13. J.G. Chakravorty, P.R. Ghosh, Advanced Higher Algebra, U.N. Dhur and Sons Private Ltd., 2018.ISBN978-3- 80673-67-7.
14. D. Stinson, Cryptography: Theory and Practice, third edition, Chapman & Hall/CRC, 2006.
15. Navita Agarwal, Prachi Agarwal, ―Use of Artificial Neural Network in the Field of Security‖, MIT International Journal of Computer Science & Information Technology, Vol. 3, No. 1, 42–44, 2013.
16. Mohammed Salih Mahdi, Nidaa Flaih Hassan Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.3 Year 2018 ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504.
17. Haykin, Simon 2004, Neural Network-A Comprehensive Foundation 2nd Ed., Prentice- Hall of India, New Delhi.
18. B.karakaya, V. Celik and A. Gulten, "Chaotic cellular neural network-based true random number generator", International journal of Circuit Theory and Applications, vol. 45, no.11, pp.1885-1897, 2017.
19. Pareek, N.K., Patidar, V. and Sud, K.K.2006. "Image encryption using chaotic logistic map. Image and vision Computing", 2006. 24(9):pp.926-934.
20. Alsafasfeh, Q.H. and A.A. Arfoa, 2011. "Image encryption based on the general approach for multiple chaotic Systems".J. Signaland Information processing, 2011. 2(3):pp.238-244.
21. Salwa K. Abd-El-Hafiz, Ahmed G. Radwan* and Sherif H. AbdEl-Haleem, 2015. "Encryption Applications of a Generalized Chaotic map", Appl.Math.Inf.Sci.9, No.6, pp: 3215-3233(2015).
22. Behnia, S.; Akhshani. A. Mafmodi, H. and Akhavan, A. 2008." A novel a lgorithm for image encryption based onMixture of chaotic maps". Chaos, Solitons & Fractals. 35(2): pp: 408-419.
23. A. A. Ghazi and F. H. Ali, ―Robust and Efficient Dynamic Stream Cipher Cryptosystem,‖ Iraqi J. Sci., vol. 59, no.2C, pp. 1105–1114, 2018.
24. N. K. Sreelaja and G. A. V. Pai, ―Swarm intelligence based key generation for text encryption in cellular Networks, in Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on, 2008, pp. 622–629.
25. S. NK and G. A. V. Pai, ―Design of Stream Cipher for Text Encryption using Particle Swarm Optimization Based Key Generation, Journal of Information Assurance and Security, 30-41 2009.
26. R. A. Ali, ―Random Number Generator based on Hybrid Algorithm between Particle Swarm Optimization (PSO) Algorithm and 3D-Chaotic System and its Application,‖ Iraqi J. Inf. Technol., vol. 8, no. 3 pp. 1–20, 2018.
27. Sheskin, D., 1997. Handbook of Parametric and Nonparametric Statistical Procedures. 2nd Edn. CRC Press, Boca Raton, ISBN-10: 0849331196, pp: 719.
28. Anirban Bhowmik, Sunil Karforma, Joydeep Dey, Arindam Sarkar, "Approximation Algorithm and Linear Congruence: A State-of-Art Approach in Information Security Issues Towards

Internet of Vehicles", Internet of Vehicles and its Applications in Autonomous Driving, Springer, Cham, 2020, pp. 149-172.

29. Thangamani, N., Murugappan, M. A Lightweight Cryptography Technique with Random Pattern Generation. Wireless Pers Commun 104, 1409–1432 (2019). https://doi.org/10.1007/s11277-018-6092-8.
30. W. Schindler and W. Killmann. Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications. In B.S. Kaliski Jr., C.K. Koc, C. Paar editors, Cryptographic Hardware and Embedded Systems—CHES 2002, Springer, Lecture Notes in Computer Science 2523, pp. 431-449, Berlin, 2003.
31. T.E. Tkacik. A Hardware Random Number Generator in In B.S. Kaliski Jr.,C.K. Koc, C. Paar editors, Workshop on Cryptographic Hardware and Embedded Systems—CHES 2002,pp. 450-453, Berlin, Germany, Lecture Notes in Computer Science 2523. Springer-Verlag Berlin Heidelberg, 2003.
32. Dey, Joydeep, Arindam Sarkar, and Sunil Karforma. "Newer post-COVID perspective: Teledental encryption by De-multiplexedperceptron." International Journal of Information Technology 13, no. 2 (2021): 593-601.
33. Sarkar, Arindam, Joydeep Dey, and Sunil Karforma, "Musically modified substitution-box for clinical signals Ciphering in wireless Telecare medical communicating systems. " Wireless Personal Communications 117, no. 2 (2021): 727-745.
34. F. D. Salimovna, Y. N. Salimovna and I. S. Z. Ugli, "Security issues in E-Education system," 2019 International Conference on Information Science and Communications Technologies (ICISCT), 2019, pp. 1-4, doi: 10.1109/ICISCT47635.2019.9011971.
35. P.K. Samanta, Dr. Sunil Karforma, "Framework for E-Education System with WDM Backbone Architecture," National Conference on Computing & System (NACCS) 2010, ISBN: 819077417-4, pp. 162-167.
36. Momeen Khan et al, "A Multi-Layered Security Model for Education Management System," (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 10, No. 12, 2019, pp. 207-211.