A framework to improve E-seva services through E-governance by using DNA cryptography

N. Srilatha
Computer Science and Engineering
JNTUAC of Engineering (Autonomous)
Pulivendula .
srilathancse@gmail.com

G.Mrali
Computer Science and Engineering
JNTUAC of Engineering (Autonomous)
Pulivendula .
muralig521@gmail.com

M.Deepthi
Computer Science and Engineering
JNTUAC of Engineering
Pulivendula .
muli.deepthi06@gmail.com

***Abstract*— the proposed frame describes two objectives one is to issue certificates through online and second is provide three level security through DNA cryptography. DNA Cryptography means converting the data to the DNA sequence. DNA is a succession comprising of four letters in order; A, C, G and T. every letter set is identified with a nucleotide. DNA can be used for store data, transmit the data and also used for computation of the data. This paper implemented 3 levels of cryptography. The receiver will apply the decryption for extracting the readable from the unreadable format. This DNA cryptography provide the security more than the other cryptography , but it takes more time complexity for generating the encoding and decoding and it has the chances to hacking the data by the hacker. So in this paper we implement the fast three level DNA Cryptography for me seva services.**

***Keywords*— DNA,LBP,DNASequence, E-Certificates,E governance.**

I. Introduction

Me seva is an online, clear and secured citizen important service facility to provide easy access to the people without any need for them to go to multiple Government offices for getting their certificates or work done It provide the certificates like income certificates Cast certificates and date of birth certificates etc..in the mean while of sending the certificate we can provide the security key by using the DNA cryptography. Here we perform cryptanalysis on the certificate who is generated by the certificate. Customer decrypt the certificate by using the secrete key.

[1].Cryptanalysis is pay role of secret writing that changes the message from structure format to unstructured data [2,3]. The structure data is easily understand by the every one, so we can convert this format into unstructured data. Cryptanalysis provide the security to our data. Now a days we have so many methods for providing the security. In Symmetric key the single key will be used at the both encoding and decoding of the cryptanalysis [4,5]. Symmetric key is provide the security for the possible attacks but it does not work for the brute force attack secret key, by using the DES algorithm we can solve this problem[7]. Asymmetric key algorithm used different keys for encoding and decoding of the data. Each part has its own key. [8] Introduces the primary cryptanalysis calculation of DNA based cryptanalysis, trailed by numerous others [9, 10]. DNA based cryptanalysis is a forthcoming branch in cryptographic research and has a wide point of view. In this review, organic idea can be thought about. Two bits can be utilized to speak to every nucleotides. The benefit of utilizing DNA cryptography is its vitality effectiveness and capacity limit [11][12]. Some of these utilization Polymerase Chain Reaction (PCR) [13], while others utilize DNA chip innovation [14]. A DNA tile gathering model has additionally been utilized for one-time cushion cryptosystems [15]. One-time cushion frameworks are particularly alluring since, if utilized accurately, they are practically unbreakable. Be that as it may, they require a vast library of DNA groupings. In DNA – BASED RSA ALGORITHM is implemented. This calculation at first prevailing with regards to beating some primary issues in "RSA". Here they were not expected to utilize genuine DNA strands to actualize cryptographic calculation, yet just to reenact a few components of the procedure of the focal authoritative opinion of sub-atomic science. In [15][16] DNA-based Cryptanalysis utilizing DNA succession for secure correspondence and key appropriation, and utilizing the concoction data of natural letters in order for steganography – Information Hiding. In Pseudo DNA cryptanalysis is utilized to defeat the breaking points of utilizing the DNA cryptography. Here they are implemented DNA-based signature scheme, a protocol for playing mental poker on the wetware, and an RNA-based zero-knowledge proof system based on solving the Sudoku problem. Providing primitives of traditional cryptanalysis since it gives an assortment of points of interest over routine silicon-based figuring ideal models. In PCR-based intensification innovation of DNA so as to tackle the key space-obliged issue that the PCR enhancement innovation of DNA has, the creators utilized a strategy for building a disorganized framework. This framework incorporates a strategic disordered guide disorganized guide. We can produce a riotous pseudo-arbitrary succession which could deal with the plaintext for disposing of the factual standards in it with the two maps. Enhancing security and the key space, and it gives an operational trial of it. In [16] characterized a one-time cushion cryptosystem utilizing DNA self-get together and demonstrated that self-get together is more proficient than PCR for creating the DNA arrangements required by our framework.. they are provide a reliability in DNA based computations and it improves previously reported methods.

The below fig shows the entire implementation of the paper. Here user directly interact with the me seva by using website and give the details. The agent scan all the adhar cards and information. All the data is true then agent provide the secrete key by using our DNA cryptanalysis. At the time of print the certificate it is used

II. BACKGROUND WORK

In this existing paper implemented a 3-Levels of security. In the principal level the key of any sought length. In the second level select four unique tenets for A, C, G, T. In the third level supplant the manage succession values with query table estimations of settled length 12.

A. *Encoding procedure:*

Step1:
First convert the readable format into unreadable format by using shift key technique. The shift key formula has given below.
Z=(Y+X) %255.

Y = Readable text

X = shift key size

Z = unreadable Text

Step2:
consider the output of step1 and convert it into ASCII format apply rule sequence table on it and then convert it into DNA sequence by the DNA conversion table.

Step3:
Implemented LBP for nucleotides A, C, G, T by using the give equation1

$$x = \sum_{k=0}^{n} (x - e)2\text{^}i$$

Eq: for conversion
Developed the rule sequence table by using the 3*3 matrix indexes of the LBP rule for nucleotides, by using the DNA conversion table and lookup table we getting the unreadable format of the original text.

B. *Decoding Procedure*

From the received text we have to reverse map to the lookup table and then to rule sequence and finally to DNA sequence.

Step1:
Received the unreadable format
Step2:
Performed the reverse map on reversed text to the lookup table and then to rule sequence and finally to DNA sequence.
Step 3:
Move the DNA sequence to 1&0 format by using order lookup table. Reverse operation is obtained text by the shift key.

III. PROPOSED METHOD

In this paper overcome the limitations of existing method i.e., more time complexity. The DNA encoding technique is used at the me seva for providing the security of the certificates. This paper proposing fast three levels DNA security.

A. Encoding

Level1:

1. Shift the readable format.

2. Get the ASCII value of the shifted text.

3. Get the binary value from the ASCII value.

4. 1's complement operation

Level2:

5. Do the LBP on the first level output.

6. Get the new binary format.

Level3:

7. Move this value to DNA sequence format by using the DNA conversion table.

8. Then obtained values send as encrypt text.

Steps for decoding process.

B. Decoding:

1. Rearrange the DNA sequence to binary format by using rule sequence.
2. Perform the LBP operation on the data.
3. Get the output of the LBP convert it into its complement.
4. Find out the segment of 8 for the binary and rearrange with respective ASCII value.
5. For the length of key shift the gained value.
6. Now readable format is gained.

Example

C. Encoding

1. Set readable format as FUN.
2. Assigned length 5 for the shift key.
3. Result of translate operation is: KZQ
4. The ASCII values of

K (75)	01001011

Z (90) 01011010

Q (81) 01010001

5. Complement of the binary values

01001011 ⟶ 10110100

01011010 ⟶ 10100101

01010001 ⟶ 10101110

6. LBP for the complement data of the changed text: The arrangement of binary values are

For K:

1	0	1
1	K	0
1	0	0

For Z:

1	0	1
0	Z	0
1	0	1

For Q:

1	0	1
0	Q	1
1	1	0

Here the data will be arranged by the row wise and get the output by the column wise.

7. LBP values for

K 11100100

Z 10100101

Q 10101111

8. DNA sequence for the LBP values by using DNA conversion table

Alphabets	Binary Representation
A	00
C	01
G	10
T	11

TABLE I. DNA CONVERSION TABLE

Conversion from LBP output to DNA sequence is:
1110010

Here take the MSB and LSB values 10 it is equal to G
1 .Remaining data is 110010 here MSB &LSB are 10 equal to G.

2 .Perform the above step until

Complete the all the b finally we get the sequence

11100100 ⟶ 10101100 ⟶ GGTA
10100101 ⟶ 11001100 ⟶ TATA
10101111 ⟶ 01101110 ⟶ CGTG

9 .Encoded Text is GGTATATACGTG.

D. Decoding

1. The encoded text is GGTATATACGTG
2. On the encoded text perform the reverse operation by rule sequence table. And perform the reverse LBP operation.
3. Do the complement operation
4. Get ASCII data

K (75) 01001011

Z (90) 01011010

Q (81) 01010001

5. Do reverse operation

K-5=F

Z-5=U
Q-5=N

5. The readable format is FUN.

SCREENSHOTS

Fig1: login and registration page

the above fig shows the 1ogin and registration page. If the user be new for our site then they register by using register or e1se if they a1ready registered use 1ogin option and get the 1ogin page.

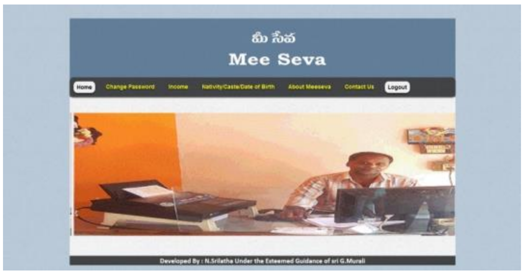
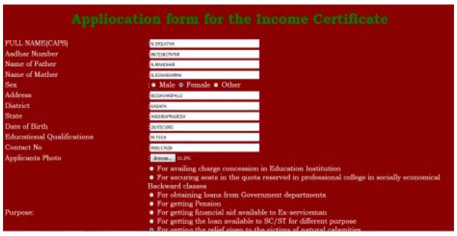

మీ సేవ
Mee Seva
Home
Change Password
Income
Nativity/Caste/Date of Birth
About Meeseva
Contact Us
Logout
Developed By : N.Srilatha Under the Esteemed Guidance of sri G.Murali

Fig2: me seva page

The above fig shows the me seva page. It contains the app1ication forms and printing options of the certificate.

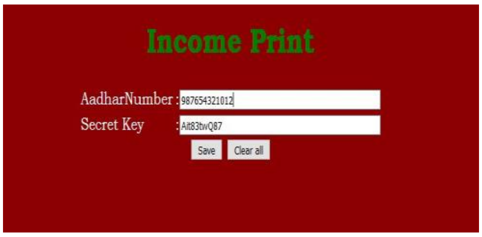


Appliocation form for the Income Certificate

FULL NAME(CAPS)	N.SRILATHA
Aadhar Number	[illegible]
Name of Father	N.MANOHAR
Name of Mather	N.ESWARAMMA
Sex	: ○ Male ◉ Female ○ Other
Address	[illegible]
District	KADAPA
State	ANDHRAPRADESH
Date of Birth	[illegible]
Educational Qualifications	M.TECH
Contact No	[illegible]
Applicants Photo	: Browse... [illegible]
Purpose:	● For availing charge concession in Education Institution ● For securing seats in the quota reserved in professional college in socially economical Backward classes ● For obtaining loans from Government departments ● For getting Pension ● For getting financial aid available to Ex-serviceman ● For getting the loan available to SC/ST for different purpose ● For getting the relief given to the victims of natural calamities

Fig 3: app1ication forms for the income certificates

The above fig shows the app1ication form for the income certificate. Here the user enter the a11 the detai1s of the adhar card number, address of him.



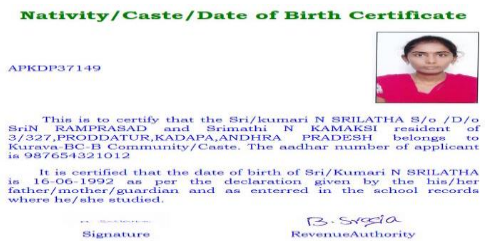
Income Print

AadharNumber : 987654321012

Secret Key : Ait83twQ87

Fig4 : income print

The above fig shows the printing page of the income certificate, caste certificate and other certificates. The page ask two numbers first one be adhar number and another be secrete number. Which be received by at the time of app1ication submit.



Nativity/Caste/Date of Birth Certificate

APKDP37149

This is to certify that the Sri/kumari N SRILATHA S/o /D/o SriN RAMPRASAD and Srimathi N KAMAKSI resident of 3/327,PRODDATUR,KADAPA,ANDHRA PRADESH belongs to Kurava-BC-B Community/Caste. The aadhar number of applicant is 987654321012

It is certified that the date of birth of Sri/Kumari N SRILATHA is 16-06-1992 as per the declaration given by the his/her father/mother/guardian and as enterred in the school records where he/she studied.

Signature

B. Srija
RevenueAuthority

Fig6: certificate

The above figure be the certificate of the native/caste/date of birth certificate.

IV. CONCLUSION

This paper describes provide a me seva certificates with a more security by using a fast DNA cryptographic technique for encoding and description. At the time of the communication the security and performance of security play a major roles. In this paper a fast DNA security technique is proposed to provide security by using the three level. In the first level is data converted into shift text and find the 1's complement. In the second level perform LBP operation and finally converted it into DNA sequence. In the decoding the levels are applied in reverse order. Here we create a web pages for applying a me seva certificates and also provide a more security to this certificates by the DNA Cryptanalysis.

V. REFERENCES

[1] Challenges of Communication in Spreading e-Govemance in Rural India.

[2] Service Oriented Architecture for E-Governance

[3] E-governance is the use of modern information and communication technologies such as internet, local area network, wide area network, mobiles, etc.

[4] Alia M.A, Public Key Steganography Based on Matching Method.

[5] Schneier B.Applied Cryptanalysis,New York John Wiley and Sons1996.

[6] Kumar, and Wollinger, Fundamentals of Symmetric Cryptanalysis *Embedded Security in Cars*, 125-143.

[7] Burke J.McDonald, and Austin Architectural support for fast symmetric key cryptanalysis.

[8] Pradeep.R kumar Reddy Reddaiah.R NagaRaju.C A review on security issues related to computer networks published in international journal of scientific Engineering and Technology and research-2015

[9] Double Layers Security by DNA Based Cryptanalysis and RSA Algorithms Smitha Mohan.M Assistant Professor Dept of IT, H Institute of Science and Technology, Ernakulam.

[10] Cui.G, Qin. L, Wang. Y and Zhang. x, An encoding scheme using DNA technology *Bio Inspired Computing:Theories and Applications,* 2008,

[11] Prabhu.D and Adimoolam.M Bi-serial DNA encoding algorithm (BDEA)

[12] GehaniA LaBeanT and Reif.J ,DNA based cryptography in *Aspects of Molecular Computing* 2950, Jonoska and Paun.G and Rozenburg.G Germany: Springer, 2004, pp.34-50.

[13] A novel encoding scheme based on DNA computing,

[14] Z.Chen and Xu One-time-pads encoding in the tile assembly model.

[15] Biological Alphabets&DNA-based Cryptography Qinghai Gao Department of Security Systems.