Cloud Security Using Hybrid Cryptography : A hybrid system that provides security to multimedia data using a hybrid encryption model composed of symmetric and asymmetric algorithms

First Author : Fidel MUMBERE VULERE [*], MSc. Information Technology

[*] Department of Management Computing, Christian Bilingual University of Congo

DOI: 10.29322/IJSRP.14.04.2024.p14825
10.29322/IJSRP.14.04.2023.p14825

Paper Received Date: 19th March 2024
Paper Acceptance Date: 24th April 2024
Paper Publication Date: 30th April 2024

Abstract **-** Data security is of utmost importance in today's world.

Especially when the data is travelling through an insecure communication network. There are symmetric key encryption techniques which use only one key for both encryption and decryption of the data. They are simple in design but can be easily cracked using brute force attacks. The entire security of such a cipher could be compromised if the attacker anyhow gets access to the keys.

On the other hand, there are asymmetric key based algorithms which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric ones but lack in time efficiency.

It is also difficult to manage such a huge base of key-pairs efficiently and safely. This paper mainly focusses on the implementation of a system capable of encryption and decryption of multimedia data (Text, Images, Videos, Audio etc.) using a hybrid model based on the amalgamation of symmetric encryption techniques such as Advanced Encryption Standard (AES) [1] and asymmetric techniques such as Elliptic Curve Cryptography (ECC).

ECC is based on the toughness of the Discrete Logarithm Problem (DLP), whose public key is short, network bandwidth is little and ability to resist to attack is strong which makes it really difficult to guess the keys. Even if the attacker gets access to any of the keys, he or she won't be in a position to decipher it in a relatively finite amount of man-years.

Index Terms- Cryptography, cryptosystem, elliptic, encryption, steganography, hashing

I. INTRODUCTION

There are a number of existing techniques such as cryptography, steganography, hashing, etc. which could provide security to the data. These techniques date back to hundreds of years where conventional techniques such as "Caeser Cipher" was used to scramble the contents of the message in order to make the confidential message unreadable or unrecognizable.

With the advancements in modern technology and easy access to the internet, traditional methods such as the Caesar Cipher was not a huge bottleneck in front of cryptanalysts or adversaries who like to break into a system or message just for the sake of pride, enjoyment or fame.

The scope of this project mainly focusses on providing security to multimedia data such as images, text files, audio, video, etc. using a hybrid encryption technique composed of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC/ECIES).

The hybrid encryption technique using a mixed encryption model based upon using the symmetric and asymmetric keys in tandem.

The existing standards provide encryption to text files at a really good stand-off but they fail to provide the same security to multimedia data such as audio, video, images etc. Even if they try to achieve it using existing [2] symmetric algorithms such as AES, DES etc., they become vulnerable to brute force attacks.

Hence a hybrid system is thought of which could provide the same security or even better using a hybrid of symmetric-asymmetric algorithms. ECC keys provide the same level of security with 160 bits as compared to RSA [3] with 1024 bits length. Hence ECC is space efficient as compared to the existing algorithms and chosen for our research work as the asymmetric key provider.

II. OVERVIEW OF CRYPTOGRAPHY ENCRYPTION TECHNIQUES

The whole literature review is focused on the following literary works being done by an array of scholars and researchers from the field of data security and mathematics. The following research/literary works are selected for review keeping in mind the traditional and conventional approaches of cryptography along with the emerging techniques.

A) **Implementation of Text Based Cryptosystem using E.C.C**

In this project, a text based Elliptic Curve Cryptosystem [5] is implemented. Each character in the message is represented by its ASCII value. Each of these ASCII value is transformed into an affine point on the Elliptic Curve (EC), by using a starting point called Pm. Transformation of the plaintext ASCII value by using an affine point is one of the contributions of this work [5].

The purpose of this transformation is twofold. Firstly a single digit ASCII integer of the character is converted into a set of coordinates to fit the Elliptic Curve. Secondly the transformation introduces non-linearity in the character thereby completely camouflaging its identity. This transformed character of the message is encrypted by the ECC technique [5].

Decryption of ECC encrypted message is itself quite a formidable task, unless we have knowledge about the private key 'nB', the secret integer 'k' and the affine point Pm1.The coordinates of the Pm1 should fit into the Elliptic Curve.

This transformation is done for two purposes. First the single valued ASCII is transformed into a (x, y) co-ordinate of the EC. Second it is completely camouflaged from the would-be hacker. This is actually intended to introduce some level of complexity even before the message is encrypted according to ECC [5].

B) **Research on Design Principles of Elliptic Curve Public Key Cryptography**

With the development of computer hardware and high performance computing Technology, RSA [9] has encountered some difficulties. In the situations, the cryptography based on elliptic curve discrete logarithm problem appears, whose public key is short, network bandwidth is little and ability to resist to attack is strong [3].

The project analyses the design principles of elliptic curve public key cryptography [3], the important contents researched in the system, the selection method of secure elliptic curve and its implementation in details.

C) **Implementation of Text Encryption using Elliptic Curve Cryptography**

A new technique has been proposed in this project where the classic technique of mapping the characters to affine points in the elliptic curve has been removed.

The corresponding ASCII values of the plain text are paired up. The paired values serve as input for the Elliptic curve cryptography [5]. This new technique avoids the costly operation of mapping and the need to share the common lookup table between the sender and the receiver.
The algorithm is designed in such a way that it can be used to encrypt or decrypt any type of script with defined ASCII values.

D) **Literature Survey on Elliptic Curve Encryption Techniques**

Preventing unauthorized access to corporate information systems is essential for many organizations. Communication security is one of the major area of interest. The data used in communication is very sensitive and needs to be protected and made abstract from intruders of system.

The recent branch of Network Security is Cryptography using Elliptic Curve Architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems [7]. ECC schemes are public-key based mechanisms that provide encryption, digital signatures and key exchange algorithms [3].

The best known encryption scheme is the Elliptic Curve Integrated Encryption Scheme (ECIES) which is included in IEEE and also in SECG SEC 1 standards.

Wireless devices are rapidly becoming more dependent on security features such as the ability to send and receive secure emails, secure Web browsing, and virtual private networking to corporate networks, and ECC allows more efficient implementation of all of these features.

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques [7].

E) **Design and Implementation of Hybrid Encryption Algorithm**

The ultimate objective of the research presented here is to develop both AES and Blowfish [2] to be low power, high-throughput, real-time, reliable and extremely secure cryptography algorithm and in addition to making estimation of both AES and Blowfish more difficult seems impossible.

The hybrid encryption scheme under consideration compares symmetric ciphers such as AES [4], DES [2], blowfish [2] and asymmetric cipher RSA [9]. RSA uses 1024 bits key and by far is the most secure cipher among the 4 discussed in the research work.

III. PROBLEM STATEMENT

Keeping all the inherent limitations of the existing technologies in mind and sensing the need of a better encryption model for

multimedia data, in terms of security as well as time, a system is proposed, which addresses the problems such as:

- **Key Size:**

The Symmetric ciphers use only a single key for encryption and decryption, hence the size of the key should be huge so that it cannot be easily guessed by any adversary using the brute force attacks. Asymmetric ciphers on the other hand use 2 keys for doing the same which impacts the memory adversely but provides better security.

- **Time Complexity:**

Complex design methodologies add up to the time complexity and simple ones provide better time complexity at the cost of security. Hence a trade-off between the two needs to be established.

- **Memory Efficiency:**

Text encryption systems offer a better memory efficiency as compared to multimedia encryption systems but lack in terms of variety, whereas multimedia encryption requires a lot of free memory space to store the keys, input files, ciphered files and the output files. Hence, again a trade-off between variety and memory needs to be established.

- **Types of Inputs Supported:**

All the literatures reviewed were all single functioned, i.e. they all support encryption for text inputs directly from the user or in the form of files containing textual information or even text messages in the form of SMS's. When it comes to high requirement multimedia inputs such as images, audio, video, graphical contents, etc. such systems lack in performance because of issues such as high memory requirement and time required to encrypt/decrypt them.

IV. TECHNIQUES USED FOR HYBRID CRYPTOGRAPHY

The proposed methodology uses a hybrid of the Advanced Encryption Standard (AES) and the Elliptic Curve Cryptography (ECC) which are explained as follows:

A. Advanced Encryption Standard (A.E.S)

The Advanced Encryption Standard [1] was proposed as a suitable replacement of the existing Data Encryption Standard (DES). It is a block cipher which takes as input a 128 bit plaintext, which is subject to an encryption with 128, 192 and 256 bit key depending upon the number of rounds i.e. 10, 12 or 14 respectively. AES [4] is different in concept from DES i.e. it is not based on the Feistel cipher [9].
Fig.1 explains the various internal rounds that take place for encryption and decryption using AES. It broadly consists of Substitution i.e. bit by bit substitution, shifting of rows i.e. transposition, mixing of columns based on modular arithmetic multiplication followed by adding of round key till n-1 rounds. Mix column round is omitted in the final n^{th} round.
After the n^{th} round a 128 bit ciphertext is obtained.

B. Elliptic Curve Cryptography (E.C.C)

The use of Elliptic Curves in public key cryptography was independently proposed by Koblitz [5] and Miller in 1985 and since then, an enormous amount of work has been done on elliptic curve cryptography. A general elliptic curve takes the general form as:

E: $y^2 = x^3 + ax + b$ ……. (1)

Where x, y are elements of GF (p) and a, b are integer modulo p, satisfying

$4a^3+27b^2 \neq 0 \pmod p$ …….. (2)

The basic EC operations are point addition and point doubling. Simple multiplication could not be found in the case of elliptic curves. A single point suppose A(x,y) on the elliptic curve could yield a resultant point B(x',y') by following a series of point addition and point doubling instead of directly multiplying the point A with a scalar, hence A = zB , where z is a scalar multiple.

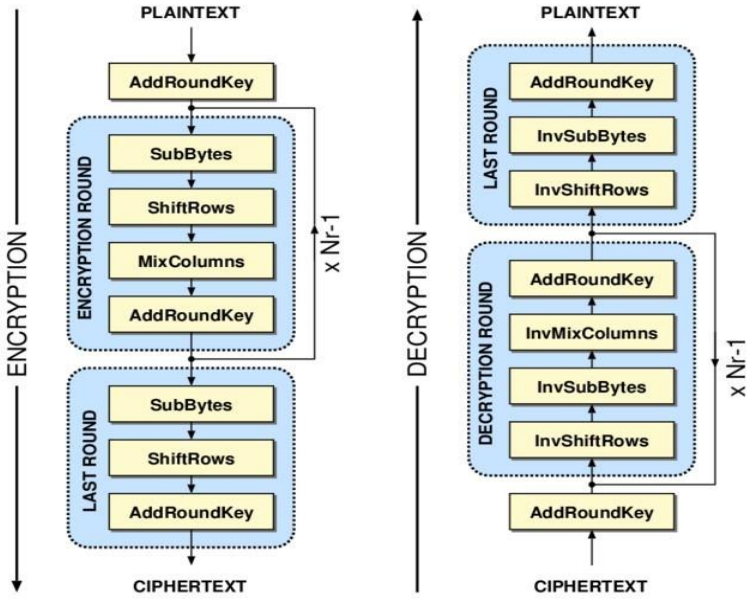


Figure 1 Advanced Encryption Standard [4]

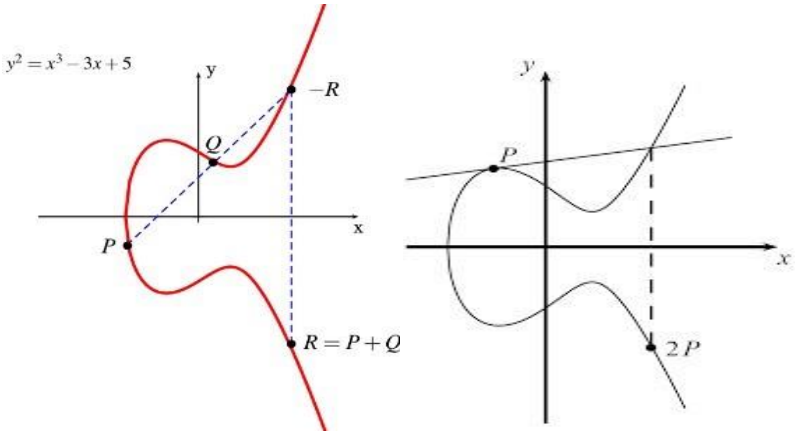


Figure 2 a) ECC Point Addition b) ECC Point Doubling

Figure 2(a) and Figure 2(b) show elliptic curve addition and doubling respectively. In Elliptic addition, a straight line joining the two points are allowed to fall on the curve in the x-y plane at point R.
The negative equivalent is obtained on the other side of the plane to produce the final result.
Similarly in point doubling, the point P itself is doubled by allowing a tangent on P to fall in the x-y plane and taking a negative intercept of the same. RSA had been the mainstay of PKC for over a quarter-century.
ECC, however, is emerging as a replacement in some environments because it provides similar levels of security compared to RSA but with significantly reduced key sizes [6] [7][8].

V. PROPOSED IDEA AND METHODOLOGY

The hybrid encryption model makes use of two cipher technologies, AES and ECC. The proposed model is based upon the robustness of the ECDLP and the simplicity of AES.

The system is intended to provide security to a variety of multimedia data ranging from text documents, images, audio, video etc. by first converting them into a base64 encoded version in text format. The same is then subjected to an initial encryption using AES, the keys for which are generated randomly. A QR code equivalent of the keys are generated in an image form which is then used by the system to extract the key in text form. This provides an extra level of security to the AES keys.

For the second level of security, the AES keys are encrypted using ECC public key, the keys for which are generated from the input base64 encoded text file. The ECC key pairs are stored at designated file-system directories.

The encrypted AES key is then further used to encrypt the base64 encoded plaintext to convert it into a corresponding ciphertext. The resultant ciphertext is already compressed and has undergone two levels of mixed encryption comprising of ECC and AES.

Such a hybrid model of encryption provides a much better level of security as compared to a single model applied individually.

The decryption process is exactly the reverse process involving a slightly complex methodology. The Methodology proposed in this research work is based on a hybrid system based on symmetric encryption using AES (128,192,256) and asymmetric encryption using ECC.

The implementation is proposed using Python as the high level programming language.

Python supports in built libraries to develop cryptographic implementations.
There are many third party organizations and developer communities like Bouncy castle and Flexi provider which provide cryptographic extensions to develop projects.

The Methodology proposed in this research work is based on a hybrid system based on symmetric encryption using AES (128,192,256) and asymmetric encryption using ECC/ECIES.

The above mentioned work is divided into various modules as follows:

a) Data Preparation

- Input conversion into base64 encoded form
- Compression of input and storing it as a text file

b) Creation of Keys and QR Code

- Creation of Symmetric AES Keys.
- Creation of ECC Private and Public Keys

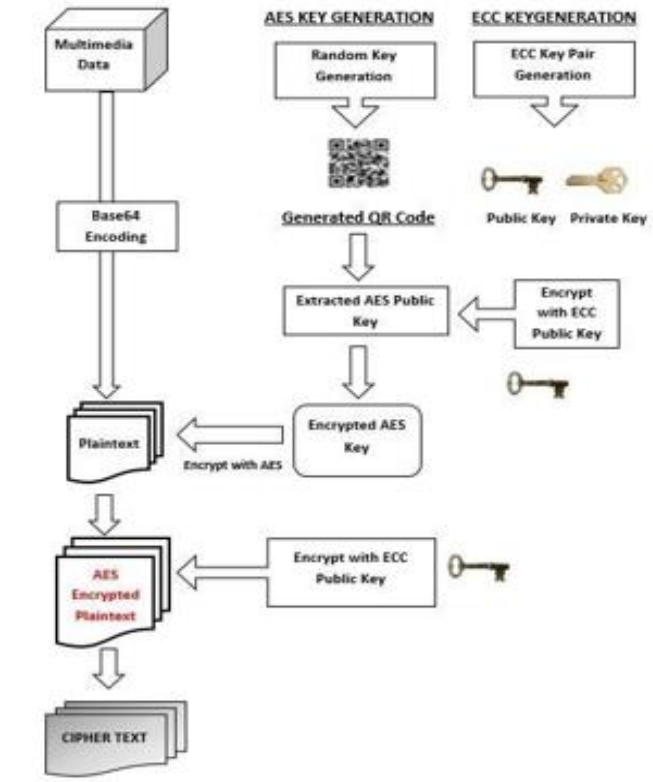


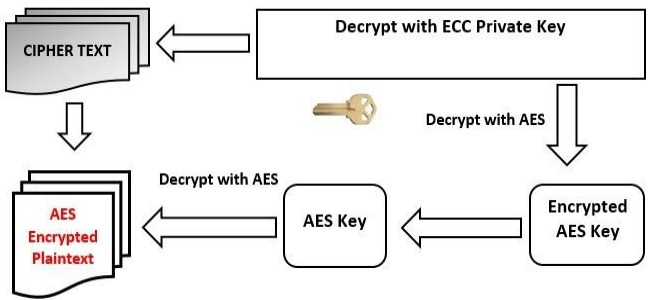
Figure 3: Encryption Process

c) Encryption Module

- Application of 1st level ECC to AES keys.
- Application of AES to input text file.
- Application of 2nd level ECC to resultant text file.
- Applying Hashing and generation of Cipher Text

d) Decryption Module

- Application of ECC private key for decryption
- Application of AES keys to recover plaintext.



10.29322/IJSRP.14.04.2023.p14825

Figure 4: Proposed Architectural Diagram for Decryption

e) Data Recovery Module

- Decompression of output file.
- Conversion from base64 form to original form

VI. RESULTS OBTAINED

The research work focusses on encrypting the multimedia data i.e. either audio, video, images, text, graphics, Pdf files etc. and storing them on the receiver's directory as an encrypted file.

The receiver in turn uses his/her private key components to decipher the encrypted data back to its original form. The following directories and their respective contents as expected are as follows:

The overall expected results are as follows:

- Overall **Time** taken for encryption and decryption is expected to go up slightly as a mixed model of encryption will be used. Time taken is expected to range between Symmetric and Asymmetric ciphers.
- Overall **Space Complexity** for storing the encrypted files and source files is expected to be reduced as compression of multimedia files are done prior to encryption and keys used are of smaller size.
- **Security level** is expected to be high as compared to the existing systems as a hybrid of symmetric and asymmetric ciphers are used.

The hybrid algorithm is implemented using a Python environment and a cryptographic library provided by Flexicore's BrainPool.

The following results are compared with the existing algorithms to generate a comparison basis for finding out the better method of choice.

The following data set is used for the encryption purpose.

Table 1. Data Set used for Text Encryption

S.No	Format	Size(in Kb)
1	.txt	118
2	.docx	153
3	.docx	196
4	.doc	312
5	.txt	868

The table below provides a comparative summary of the various methods used.

Table 2. Comparative Summary of Existing and Proposed Method [9]

Size(In Kb)	Time (In Sec)				
	AES	**DES**	**RSA**	**ECC**	**Hybrid**
118	1.7	3.2	10	1.20	1.135
153	1.6	3	7.3	1.04	0.808
196	1.7	2	8.5	1.23	1.03
312	1.8	3	7.8	1.24	0.917
868	2	4	8.2	1.17	0.937
Avg. Time	**1.76**	**3.04**	**8.36**	**1.17676**	**0.9654**
Avg. Size	**329.4**				
Speed	187.16	108.36	39.41	279.92	341.21

The following Fig.5.1 shows a graphical representation of the comparative analysis between the existing techniques and the proposed hybrid methodology.

It can be seen that the proposed technique is many folds faster than the traditional existing techniques. The closest competitor in terms of speed is ECC which uses 384 bit keys whereas the proposed technique uses 160 bit ECC keys and 128 bit AES keys.

The fastest among the symmetric algorithms comes out to be AES which is nearly half in speed as compared to the proposed hybrid method.

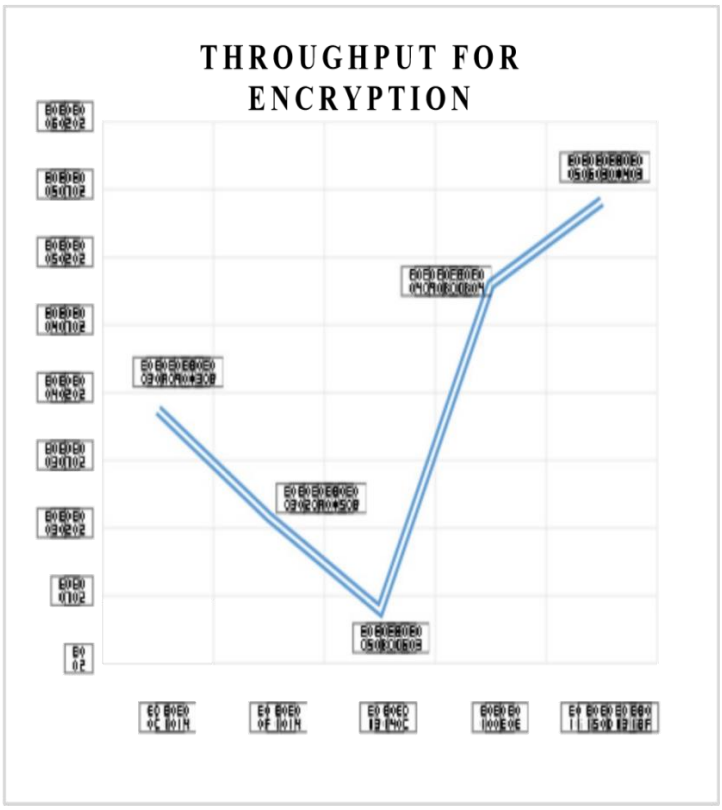


Figure 5.1 Graphical Comparative Analysis

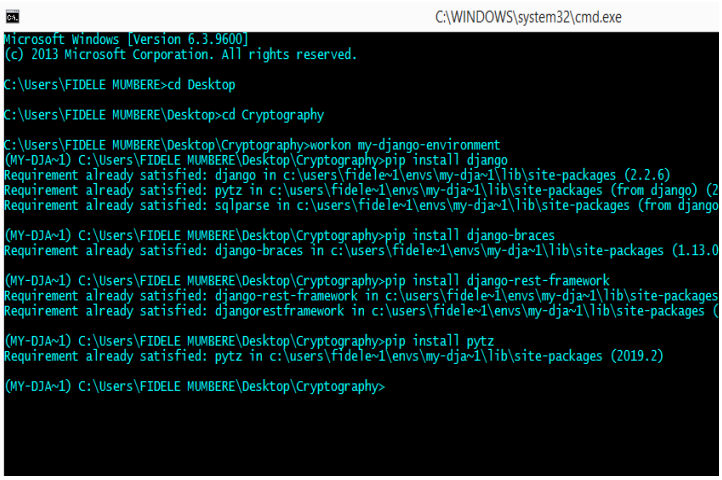


Figure 5.2 Requirements for python virtual environment

Software requirements installed to run the cryptography implementation code in a **python virtual environment** (Django, djangorestframework, django-braces, pytz already satisfied.)

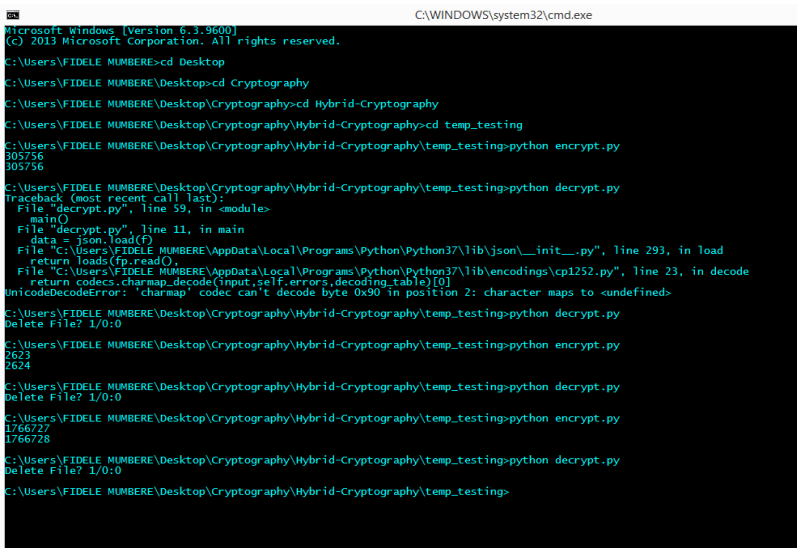


Figure 5.3 Testing the encryption and decryption of files

Encryption and decryption of files (image, text, audio and video) in figure 5.3 and displaying the encrypted and decrypted files.

Home page of the website of the cloud security cryptography system is as below:

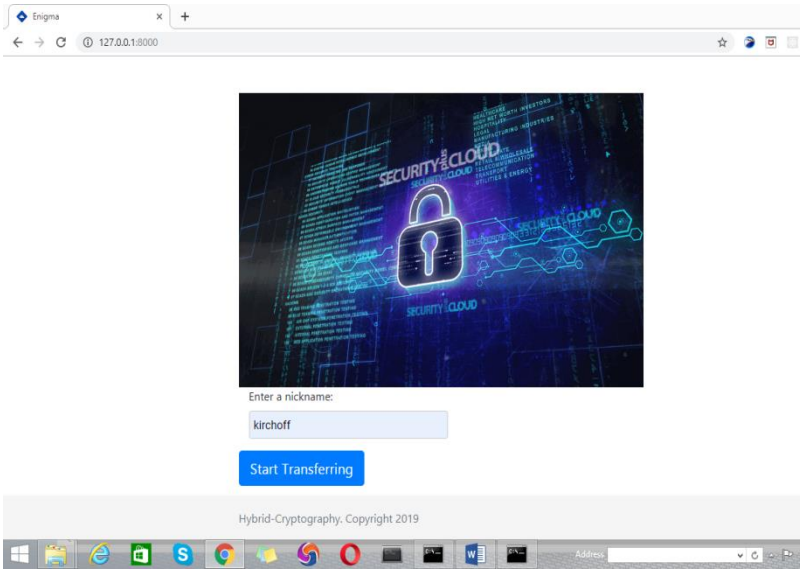


Figure 5.4 Home page of the website

VII. CONCLUSION AND EXTENSIONS

To conclude, it can be said that the current implementation has been tested on text files and the results obtained so far are very motivating because of the speed gains over the existing techniques.

The current implementation can also be used for images, audio and video encryption with minor changes in the implementation design to compress the multimedia source files before and after encryption.

The implementation could be used in applications requiring encryption of multimedia data at a rapid pace. The same implementation could be used in a network to encrypt the files travelling through it for example, attachments travelling through an email could be secured using the hybrid encryption along with the existing email security provided by the mail server or using it alone.
Because of its high speed gains over the existing techniques, the same implementation could be used for handheld devices by doing some minor changes in the implementation framework.

REFERENCES

[1] Daemen, Joan, Rijmen, Vincent. (March 9), AES Proposal: Rijndael. National Institute of Standards and Technology 2003; p. 1. Retrieved 21 February 2013.

[2] Jawahar Thakur, Nagesh Kumar. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering* December 2011; vol 1(2), p.6-12

[3] R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* 1977; p. 120-126

[4] Wikipedia.org, "Advanced Encryption Standard", https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[5] S.M.Celestin, V.K.Muneeswaran, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography. *IEEE International Conference on Advanced Computing* Dec 2009; p. 82-85.

[6] HafidMammass and FattehallahGhadi, Implementation of Smartcard Personalization Software. *International Journal of Future Generation Communication and Networking* 2012; vol 5(4).p.39-54

[7] F. Amounas and E.H. El Kinani, A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin ½ Matrices. *International Journal of Information & Network Security (IJINS)* 2013; vol 2(3), p. 190-196.

[8] Md. Zaheer Abbas, Dr. JVR Murthy, Authenticated And Policy - Compliant Source Routing. *International Journal of Engineering Research and Applications (IJERA)* 2012; vol 2(3), p.1347-1352.

[9] B. Padmavathi, S. Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique," *International Journal of Science and Research (IJSR)*, India Online ISSN: 2319-7064; Volume 2 Issue 4, April 2013; p.170-174

ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible and whose constant guidance and encouragements crown all efforts with success.
I take this occasion to give thanks and praise to the Almighty God for blessing me with His grace, strength and determination to bring this research project to a successful culmination.
My thanks go out to all those who helped through their comments, feedback, edits or suggestions.
I would like to thank the team of dedicated lecturers and the whole establishment of Christian Bilingual University of Congo. The guidance and counsel they have always shared with us will carry a long way in my personal and academic research development. I will have the honor of working courageously in the academic research field in the near future.
I would like to express my obligation to my faculty colleagues and animators Dr. Rebecca Wasingya(Faculty Coordinator), CT. Papy Angoezi and CT. Bakwanamaha Patrick for their valuable inspiration and constructive suggestions that were so helpful to me throughout the research project.
Special thanks go to my beloved parents Katsongo Kamate and Masika Dikla and family for the moral and financial support they have accorded me throughout my research study project.
I have benefited from the friendship, guidance and the knowledge you have all shared with me.

AUTHORS

First Author – MUMBERE VULERE FIDEL,
Master of Science in Information Technology
(MSc. Information Technology - Data Engineering),
Assistant Researcher & Visiting Lecturer at Christian Bilingual University of Congo.
E-mail address : mumfidel@gmail.com