Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 10, October 2020, pg.83 – 94

HYBRID ENCRYPTION OF BIG DATA SECURITY USING IMPROVED ELLIPTIC CURVE CRYPTOGRAPHY

Dr. B. Arputhamary
Associate Professor, Department of Computer Application, Bishop Heber College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, India
arputhambaskaran@rediffmail.com

A. Benita
Department of Computer Science, Bishop Heber College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, India
benshs1996@gmail.com

DOI: 10.47760/IJCSMC.2020.v09i10.011

Abstract— In terms of identifying the attacker, the Big Data environment helps resolving cyber security problems. There are big data security concerns as well as safety issues that the analyst must understand. The security of confidential data has long been a serious concern, and as a result, data security is in huge demand. Data is considered an important aspect of an asset and must be protected. Data Protection comprises data integrity, data authenticity, data confidentiality, and then some. Data is prone to possible security risks despite several measures for protecting data including encryption, decryption, and compression. Cryptography is an art and science that encodes messages to make them unreadable in order to achieve secrecy. The data is translated from a readable format known as plain text to an unreadable format known as cypher text, and vice versa. Based on various techniques, there are different types of cryptographic algorithms proposed over the years. These methods use different techniques to implement cryptography's fundamental features, i.e. to conceal the data from unauthorised users. A hybrid cryptographic technique is proposed in this paper to enhance data protection during network transmission, and its implementation and results are published. The proposed secure cryptographic technique promises to use the Enhanced ECC and AES technologies to include the highly secure cypher generation technique. Using JAVA technology, the implementation of the proposed technique is given and its efficiency in terms of space and time complexity is calculated and compared with conventional ECC cryptography. During comparative performance analysis, the proposed cryptographic technique established the successful and enhanced cypher text.

Keywords: Bid Data, Cryptography, Encryption, Decryption, Elliptic Curve Cryptography (ECC), AES.

I. INTRODUCTION

Big data is large data sets which conventional processing systems are unable to analysis and handle. Data sets are growing to sizes that conventional ITs can no longer support the size, volume and growth of data in big data. It is difficult to handle and garner profit from it. Acquisition, storage, searching, sharing, analytics, and data visualisation are the main difficulties. As the data set evolves, the procedures involved in exploiting the data are also changing. Business intelligence, analytics and data mining are also synonymized with it. The distinction between the two is that Big Data is about inductive statistics and descriptive statistics are about market analytics.

Big data is not something that has arisen in recent days, but it has seen an immense amount of knowledge documented only in the last two years. Big Data has been researching massive and complex data for drug creation, physics modelling, and other areas of analysis, clinging to the fields of science and medicine. And now, from these beginnings, Big Data is now beginning to grow in numerous areas.

Value extraction is simpler than before from the data collection. Big Data is full of challenges, from the technical to the conceptual to the operational, any of which can derail the ability to discover value and take advantage of what Big Data is all about. Big data has challenges extending from technical to conceptual and operational, hampering the ability to extract value better and leveraging the big data definition.

II. CRYPTOGRAPHY

Cryptography plays an essential role in data protection. Crypto means secret anything. In the field of vision of unapproved individuals, this is the analysis and use of protected correspondence methods. It is dedicated to the creation and analysis of protocols which do not allow data exchanged between two objects to be received by malicious third parties, and thus aspects of data security [1][3].

Following are the classified categories of Cryptography:

- Hash functions
- Symmetric key cryptography and,
- Asymmetric key Cryptography

2.1 Symmetric-key: These are cryptographic algorithms that encrypt plain text and decrypt encrypted text using the corresponding cryptographic keys. The keys may be indistinguishable, or you can make a simple shift between two keys, called a common key or mutual secret encryption. A single key for encrypting and decrypting traffic [3] is used with symmetric encryption.

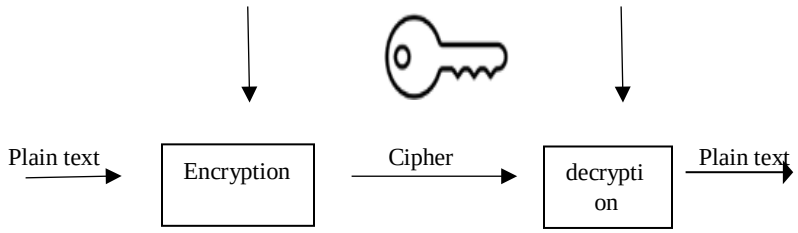

Fig. 1: Symmetric key, a single key for encrypt and decrypt

2.1.1 Advanced Encryption Standard (AES): It is measured to be at least six times faster compared to DES, one of the most commonly used symmetric encryption algorithms. The main size used in DES was too small and that led to a replacement being created. In recent times, with increasing computational capacity, it has been found vulnerable to potential key search attacks. A triple DES algorithm was suggested as an alternative, which was then dropped due to its slow computing speed [12].

Asymmetric key: Asymmetric keys are distinct from symmetric keys, operating on the idea of two separate keys, a private key that during contact is kept confidential to the owner, and a public that can be widely circulated by users. To obtain unidirectional functions, the generation of these key pairs depends heavily on mathematics-based cryptographic algorithms. During the decryption and encryption method, this encryption technique uses different keys; thus, any user may encrypt data using the available encryption key for the public key [3].

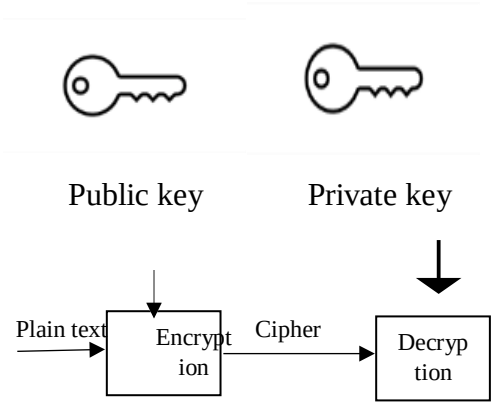

Fig. 2: Asymmetric encryption, (public-key exchange)

Elliptic Curve Cryptography (ECC): ECC is a method of public-key encryption algorithm described on the basis of the elliptic curve algebraic structure spanning finite fields. To provide a comparable degree of security, it requires a comparatively smaller key than non-ECC encryption. (The equivalent protection obtained by RSA 3072-bit crypto is 256-bit ECC protection).

This thesis is intended to provide an enhanced security service in Big data using an enhanced Elliptic Curve Cryptography algorithm for securing user data. The thesis is also extended to present both the theoretical and empirical results of the proposed improved elliptic curve based public key cryptography to prove that the model is better than the traditional AES based schemes in terms of encryption, decryption time and key sizes.

III. RELATED WORK

Thu Yein Win et al. [2017] proposed a novel big data-based security analytics approach to detecting advanced attacks in virtualized infrastructures. Network logs as well as user application logs collected periodically from the guest virtual machines (VMs) are stored in the Hadoop Distributed File System (HDFS). (Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing)

Thangapandiyan et al. [2018] proposed provide to a privacy to sensitive data, a Modified Elliptic Curve Cryptography (MECC) algorithm. The proposed algorithm generates separate key for all admins and users to access the data. The data is encrypted and decrypted by utilizing the similar MECC algorithm. Whenever the users and other admins want to access the cloud data, they are verified for their identity. After positive verification, the requesters are provided with attributes. The receivers execute the MECC algorithm and generate private key for decrypting the data with these attributes. This ensures high degree of data encapsulation in cloud computation. Performance comparison between the proposed and conventional schemes are carried out and observed that the MECC algorithm is highly secure than other conventional schemes. (Enhanced Cloud Security Implementation using Modified ECC Algorithm)

Vishal Prakash et al. [2019] created new hybrid cryptography using one well-trusted fusion of RECTANGLE SPECK & LED. In the analysis work implementation of our hybrid system will generate variable size key with minimum time complexness and better security that is with competence suited in real time cryptography. A solely approved person can access the information. During this context, a key is the fusion of the various specialists for taking a final decision. (A New Model of Light Weight Hybrid Cryptography for Internet of Things)

Vinay Poduval et al. [2020] proposes the working of the hybrid cryptography and image steganography algorithms for the secure storage of files on the cloud. This technique helps in achieving higher efficiency and better security due to the use of multiple algorithms for the encryption/decryption process. Added work on this paper, the use of 3-DES algorithm has been done for the encryption purpose for getting suitable results and achieving higher security for the transmitted data. High level security of data is required in banking and private sectors where the proposed system can be used.

Manjula Y et al. [2016] proposes encryption of data happens before data transmission to ensure data security. The Hybrid Encryption Model is utilized for the encryption of data. The encryption is finished by data cleaning for data normalization and data de-duplications. Duplication Data detection technology first isolates the data document into a gathering of data squares, assesses fingerprints for each data square, at that point utilizes fingerprints as keywords for playing out a Hash search. The encryption model uses ECC encryption for encoding the Hash table and the Symmetric encryption method to re-encryption the enormous data handled after the primary period of encryption.

IV. ECC ALGORITHM FOR ENHANCING BIG DATA

In this analysis, the AES algorithm is implemented for authentication purposes and the Enhanced ECC algorithm is used in Bigdata storage for file (document) encryption. Unauthorized users can be blocked, password forgotten and hidden no. is sent to a personal email address along with file encryption, upload, download and decryption. The first goal of the proposed work is to make the system safe so that only approved users can log in to the Bigdata. If any unauthorised user tries to access our data, they can easily monitor and permanently block the device's IP and even MAC address from where they attempt to access our data. Secondly, using the ECC algorithm, the file sharing in data is fully safe and difficult to decrypt and make the packets move securely on the network using ECC, so that any hacker does not intercept or decrypt any packet.

Figure 3 shows the complete working for proposed system. It describes that after registration if any user is trying to login and if password is wrong or MAC address is wrong for 5 times the account was blocked. Figure 4 describes the possible operations for proposed system; these operations can be applied on document (files) for their security.

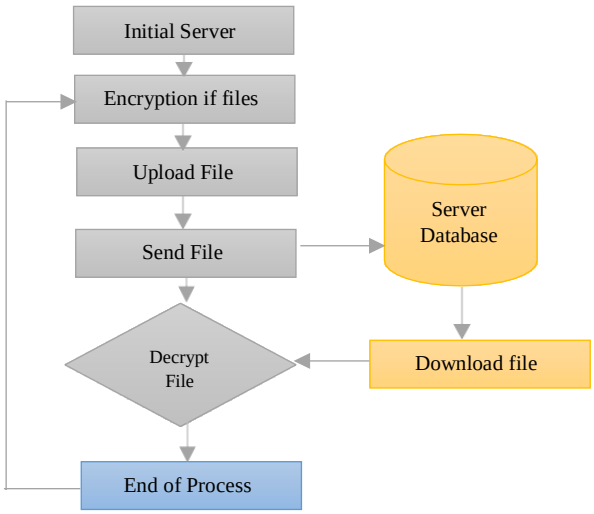

Figure 3. The flowchart for file process.

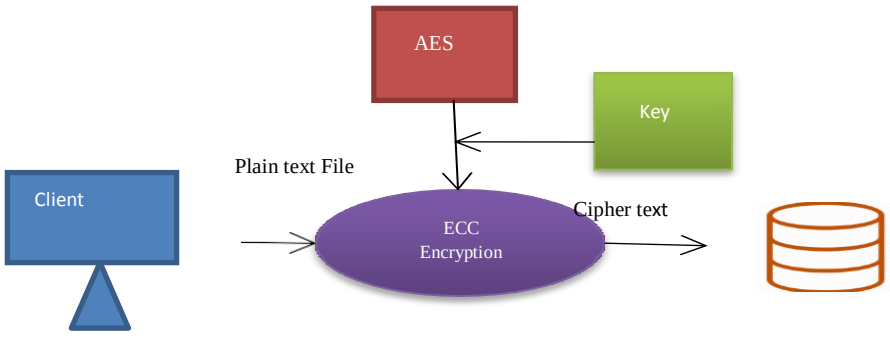

Figure 4. Proposed Architecture

V. ELLIPTIC CURVES

First and foremost: what is an elliptical curve? An excellent and full description is given by Wolfram MathWorld. But an elliptical curve would simply be the set of points defined by the equation for our aims:

$$y^2 = {}^3 + ax + b$$

Where 4a3+27b2≠0 (this is required to exclude singular curves). The equation above is what is called Weierstrass normal form for elliptic curves.

A. Encryption

- Let "m" be the message that we are sending.
- Here have to represent this message on the curve.
- Consider 'm' as the point 'M' on the curve 'E'.
- Randomly select „k" from $[1 - (n - 1)]$
- Cipher texts will be generated after encryption, let it be C1 and C2.
- $C1 = k * p$
- $C2 = M + k * Q$

B. Decryption

- The message "M" that was sent is written as following equation,
- $M = C2 - d * C1$

VI. ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard (AES) is a cypher symmetrically used by the US administration to secure sensitive information from symmetrical block encryption. AES is worldwide used to encrypt confidential data in software and hardware. For state information safety, cyber safety and electronic data security, this is critical.

The NIST began developing AES in 1997, by announcing the need for an alternative to the Data Encryption standard, which was already becoming vulnerable to attacks by raw powers.

NIST said the new, advanced encryption algorithm will be unclassified and "will protect government sensitive information well into the 21st century." It was intended to be simple to instal in hardware and software, as well as to provide decent protection against a range of attack strategies in restricted environments, such as an intelligent card.

AES has been developed to provide additional voluntary, free use for the US government through public or private, commercial or non-commercial encryption programmes. However, the constraints created by US export control relate to non-governmental organisations selecting AES.

VII. ECC WITH AES

This section contains the working with elliptic curves which are defined over Zp. These are often called the prime curves and can be far simpler to work with as here can reduce modulo p at each stage. Suppose we have an elliptic curve, E, over Zp. In this case we have a cubic equation in which the variables and coefficients take values on the set of integers 0, 1, ... (p − 1) and all calculations are performed modulo p. y 2 ≡ x 3 - Ax - B (mod p) here write Ep(A, B) for the set of integers (x, y) that satisfy the above equation, together with a point at infinity, ∞.

The set E11(1, 6) is the set of integers (x, y) that satisfy

y 2 ≡ x 3 - x - 6 (mod 11)

Here can see that (x, y) = (7, 9) is in this set as 9 2 (mod 11) = (73 + 7 + 6) (mod 11)

81 (mod 11) = 356 (mod 11) ⇐⇒ 4 = 4

To find all the points in E11 (1, 6) here find all the possible values x 3 + x + 6 (mod p) and then see what values of y 2 will match. There are 11 choices of x, the integers {0, 1... 10}. Subbing these values in turn into the cubic and reducing modulo 11 will give us the possible values of y 2:

x = 0 =⇒ RHS = 6 x = 6 =⇒ RHS = 228 ≡ 8

x = 1 =⇒ RHS = 8 x = 7 =⇒ RHS = 356 ≡ 4

x = 2 =⇒ RHS = 16 ≡ 5 x = 8 =⇒ RHS = 526 ≡ 9

x = 3 =⇒ RHS = 36 ≡ 3 x = 9 =⇒ RHS = 744 ≡ 7

x = 4 =⇒ RHS = 74 ≡ 8 x = 10 =⇒ RHS = 1016 ≡ 4

x = 5 =⇒ RHS = 136 ≡ 4

So we can see that the possible values of y 2 are {3, 4, 5, 6, 7,
8, 9} i.e. y 2 cannot be 0,1,2 or 10. Next examine the 10 possible values of y and identify which values of x they could be paired with to give a point on the curve.

y = 0 ⇒ y 2 = 0 ⇒ No Points y = 6 ⇒ y 2 = 36 ≡ 3 ⇒ x
= 3

y = 1 ⇒ y 2 = 1 ⇒ No Points y = 7 ⇒ y 2 = 49 ≡ 5 ⇒ x
= 2

y = 2 ⇒ y 2 = 4 ⇒ x = 5, 7, 10 y = 8 ⇒ y 2 = 64 ≡ 9 ⇒ x
= 8

y = 3 ⇒ y 2 = 9 ⇒ x = 8 y = 9 ⇒ y 2 = 81 ≡ 4 ⇒ x
= 5, 7, 10

y = 4 ⇒ y 2 = 16 ≡ 5 ⇒ x = 2 y = 10 ⇒ y 2 = 100 ≡ 1
⇒ No Points

y = 5 ⇒ y 2 = 25 ≡ 3 ⇒ x = 3

E11(1, 6) = {(2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2),
(7, 9), (8, 3), (8, 8), (10, 2), (10, 9), ∞} An m-file, PC.m, to
find and plot all the points on a prime curve was constructed and is stored. This m-file takes as its inputs, A, B and p and produces two vectors X, Y which contain all the points (x, y) that lie on

$y2 = Ax + B$ (mod p). When run on this example it verified that we had found all the points in E11(1, 6) and plotted the graph below. Here can see that the points are symmetric about the line y = 5.5

Here can perform the elliptic curve addition operation on prime curves; however, here reduce modulo p at each step. For example, still considering E11 (1, 6):

If P = (8, 3) then we know that −P = (8, −3). Working modulo 11 we see that −P = (8, 8) which is also a point in E11(1, 6).

Let P = (8, 3) and Q = (3, 5). Then to find R = P + Q: m = (5 – 3) / (3 – 8) = 2/ −5 ≡ 2 /6

= 1 /3 = 1 × 4 = 4

The penultimate step involved taking the multiplicative inverse of 3 in Z11. Now proceed to show that

xR = 42 − 8 − 3 = 5, yR = 4(8 − 5) − 3 = 9 So in E11(1, 6) we
find (8, 3) + (3, 5) = (5, 9). • Again, let P = (8, 3). To calculate 2P = P + P:

m = (3(82) + 1) / (2 ∗ 3) = 193 /6 ≡ 6/ 6 = 1 (mod 11)

Then x2P = 12 − 2(8) = −15 ≡ 7 (mod 11)

y2P = 1(8 − 7) − 3 = −2 ≡ 9 (mod 11)

So in E11 (1, 6) we find 2(8, 3) = (7, 9).

The earlier m-file for performing elliptic curve addition was modified for use with prime curves. It now reduces modulo p at each stage using mod function and find the inverse of elements so the final answer is an element on a prime curve. It contains the same inputs and outputs as m but the user must input p in addition. It makes use of the m-file inseam which is stored. This m-file takes as its inputs a number N and a prime p and outputs the inverse of N in the group Zp. The m- file m was used to calculate the remaining entries in the addition table overleaf. In show that (2, 7) is a generator of this group and so it is isomorphic to Z13.

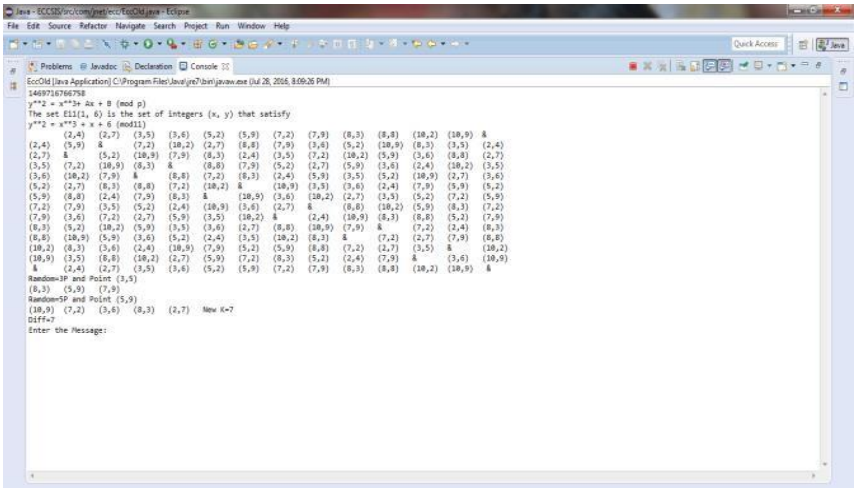

Figure 5. Key Generation output point

A Big data to build networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A Big data consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most data are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered.

A. Key Comparison for Standard ECC and Improved ECC Algorithm

Fig 6 represents the Key comparison Time chart of the resources with respect to expected completion time of tasks.

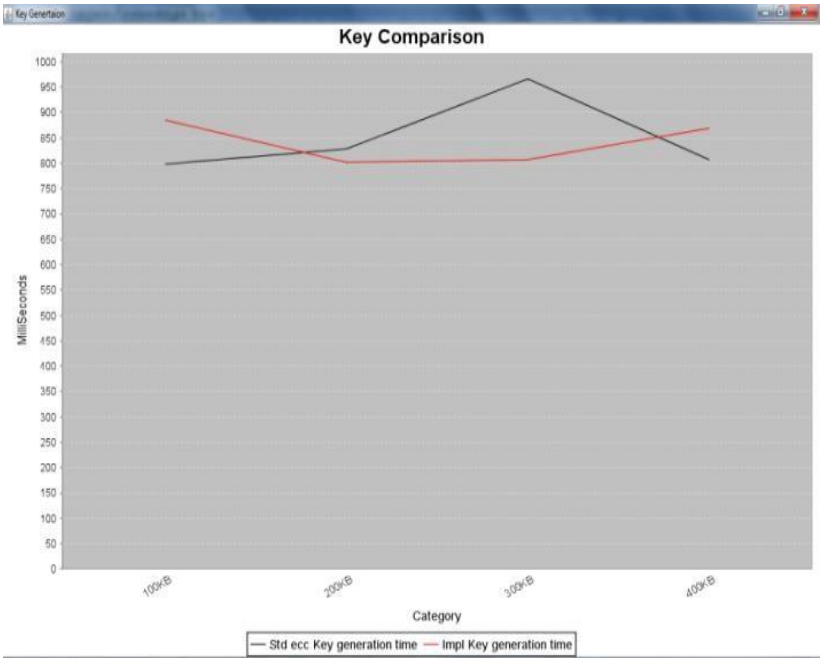

Figure 6. Key Comparison

B. *Encryption Time Comparison for Standard ECC and Improved ECC Algorithm*

Fig 7 represents the Encryption Time chart of the resources with respect to expected completion time of tasks.

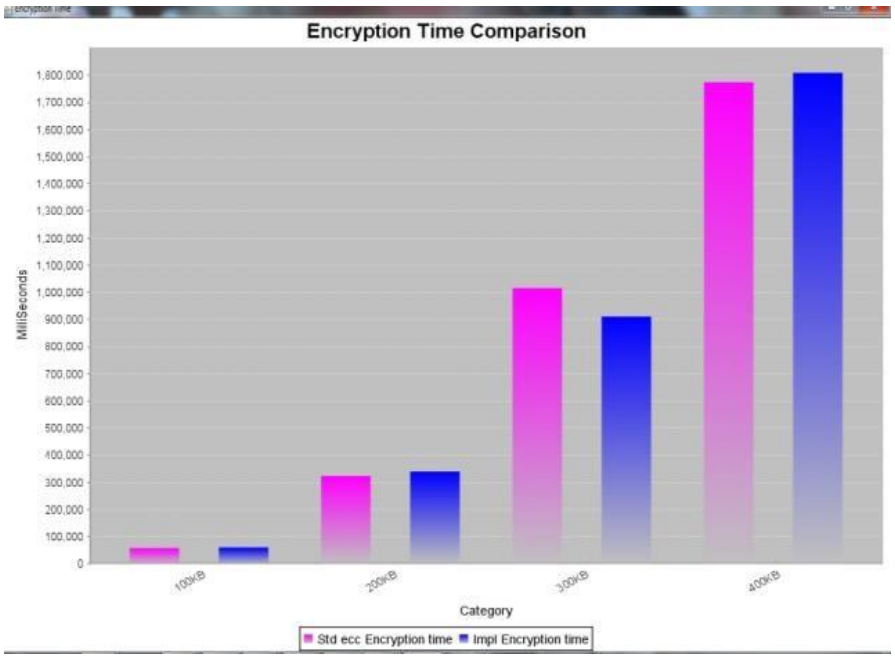

Figure 7. Encryption Time

C. *Decryption Time Comparison for Standard ECC and Improved ECC Algorithm*

Fig 8 represents the Decryption Encryption Time chart of the resources with respect to expected completion time of tasks.

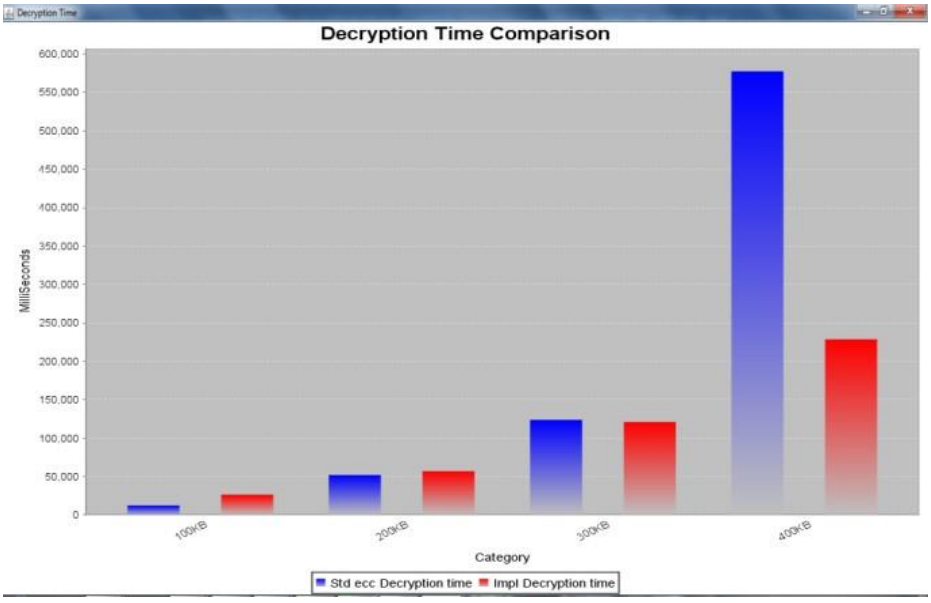

Figure 8. Decryption Time

D. Summary

This section contains the working with elliptic curves which are defined over Zp. These are often called the prime curves and can be far simpler to work with as here can reduce modulo p at each stage.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

A. Conclusion

Data has become more important as the methods which are used to ensure security not only need to be strong and efficient but should be easy to implement and execute. However, several challenges still weigh down the technology. Resolving security problems with Big data is one such major challenge. It requires an adequate understanding of both the security issues in data implementation as well as the solutions presently available to address these. The security model is used to improve security without degrading the performance of the system. Main goal of future improvement is providing more security by using more secure algorithm whose security can't be broken.

Simulation results shows that AES algorithm is best for authentication and ECC algorithm used for security has better performance than other techniques. Since ECC has not any known security weak points till now, it can be considered as an excellent standard encryption algorithm. The experimental results reveal that the proposed method offers better performance over previous work.

B. Future Enhancement

In future here can use ECC algorithm for securing audio and video data. Because, In the area of security, research area of speech is very wide. The Android platform of Smartphone's is a powerful platform and is used in 80% of Smartphone's today. The sensors that come with the mobile devices further give a context to cloud applications and opens up a new set of possibilities.

References

[1]. Izhar, Shariqua, Anchal Kaushal, Ramsha Fatima, and Mohammed A. Qadeer. "Enhancement in data security using cryptography and compression." In 2017 7th International Conference on Communication Systems and Network Technologies (CSNT), pp. 212-215. IEEE, 2017.

[2]. Devi, T. Rajani. "Importance of cryptography in network security." In 2013 International conference on communication systems and network technologies, pp. 462-467. IEEE, 2013.

[3]. En.wikipedia.org. (2020). Data Encryption Standard [online] Available at: https://en.wikipedia.org/wiki/Data_ Encryption_Standard [Accessed 25 Mar. 2020].

[4]. Win, Thu Yein, Huaglory Tianfield, and Quentin Mair. "Big data-based security analytics for protecting virtualized infrastructures in cloud computing." IEEE Transactions on Big Data 4, no. 1 (2017): 11-25.

[5]. Thangapandiyan, M., PM Rubesh Anand, and K. Sakthidasan Sankaran. "Enhanced cloud security implementation using modified ECC algorithm." In 2018 International Conference on Communication and Signal Processing (ICCSP), pp. 1019-1022. IEEE, 2018.

[6]. Prakash, Vishal, Ajay Vikram Singh, and Sunil Kumar Khatri. "A New Model of Light Weight Hybrid cryptography for Internet of Things." In 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 282-285. IEEE, 2019.

[7]. Vinay Poduval, Ashish Koul, Daniel Rebello, Karunesh Bhat, Revati M. Wahul. "Cloud based Secure Storage of Files using Hybrid Cryptography and Image Steganography", International Journal of Recent

Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020.

[8]. Manjula, Y., and K. B. Shivakumar. "Enhanced secure image steganography using double encryption algorithms." In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 705-708. IEEE, 2016.

[9]. Ghosh, Suman Kalyan, Sachin Rana, Anushikha Pansari, Joydev Hazra, and Satarupa Biswas. "Hybrid Cryptography Algorithm For Secure And Low Cost Communication." In 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), pp. 1-5. IEEE, 2020.

[10]. Viswanath, G., and P. Venkata Krishna. "Hybrid encryption framework for securing big data storage in multi-cloud environment." Evolutionary Intelligence (2020): 1-8.

[11]. Timothy, Divya Prathana, and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." In 2017 International conference on microelectronic devices, circuits and systems (ICMDCS), pp. 1-5. IEEE, 2017.

[12]. Biswas, Chitra, Udayan Das Gupta, and Md Mokammel Haque. "An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography." In 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), pp. 1-5. IEEE, 2019.

[13]. AbdElminaam, Diaa Salama. "Improving the security of cloud computing by building new hybrid cryptography algorithms." International Journal of Electronics and Information Engineering 8, no. 1 (2018): 40-48.

[14]. Hoobi, Mayes M. "Efficient Hybrid Cryptography Algorithm." Journal of Southwest Jiaotong University 55, no. 3 (2020).

[15]. Pooja, and R. K. Chauhan. "Triple phase hybrid cryptography technique in a wireless sensor network." International Journal of Computers and Applications (2020): 1-6.

