JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

A Review on Secured Network with Cryptographic Modelling

A. Suresh[1*], M. Hemamalini[2]

[1]Department of Computer Science, A.V.C College (autonomous),India
[2]Department of Computer Science, A.V.C College (Autonomous), India

Corresponding Author: maliniavcce@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—**In information network security is one of the most important elements because it is responsible for providing security to all information passed through network devices. System security includes the approval of access to information in a system and it will controlled by the system administrator. Cryptography gives secure correspondence within the sight of vindictive outsiders-known as foes. Cryptography is the way toward changing over standard plain text into cipher text. There are two sorts of cryptography they are symmetric and asymmetric. In symmetric frameworks use a similar key (the mystery key) to scramble and unscramble a message. In asymmetric frameworks use an open key to scramble a message and a private key to decode it. Utilization of uneven frameworks upgrade makes secure correspondence. Asymmetric frameworks incorporate RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography). The proposed framework utilizes AEDA calculation for information encryption as a result of its significant points on high security, bring down CPU time and less memory use. In AEDA Encryption and Decryption techniques can just scramble and decode a pixel value. The Encoding (converting message to a point) and Decoding (changing over a point to a message) are imperative capacities in Encryption and Decryption in AEDA.

***Keywords*-**Cryptography, Symmetric Key, Asymmetric Key, ECC, RSA, AEDA.

I. INTRODUCTION

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity [1].
The Figure 1 shows the classical encryption and the terms in the diagram are defined as:

- Plaintext: original message
- Ciphertext: coded message
- Enciphering or encryption: the process of converting from plaintext to ciphertext
- Deciphering or decryption: the process of restoring the plaintext from the ciphertext.

Many encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: Symmetric-key (also called secret-key) and Asymmetric-key (also called public-key) encryption.

Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption [2].

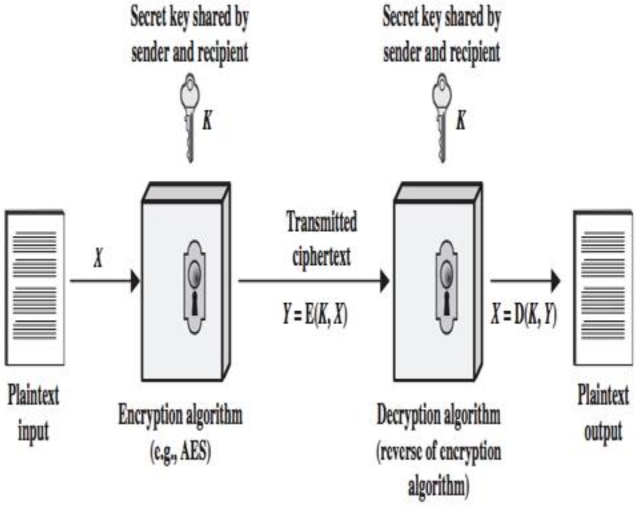
Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1: Classical Encryption

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together [3][4].

ASYMMETRIC KEY CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC)

ECC was introduced by Victor Miller [5] and Neal Kolbitz as an alternative to established public key systems such as RSA [9]. In 1985, they proposed a public key cryptosystems analogue of ElGamal encryption schema witch used Elliptic Curve Discrete Logarithm Problem (ECDLP) [7]. Elliptic curve cryptosystems (ECCs) include key distribution, encryption algorithms. The key distribution algorithm is used to share a secret key and the encryption algorithm enables confidential communication. ECC is based on the addition of rational points on a chosen elliptic curve.

One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. Elliptic curves are applicable for the encryption, digital signatures, pseudo-random generators and other tasks. It is also used in several integer factorization algorithms that have applications in cryptography.

An elliptic curve is not an ellipse (oval shape), but is represented as a looping line intersecting two axes (lines on a graph used to indicate the position of a point). ECC is based on properties of a particular type of equation created from the mathematical group (a set of values for which operations can be performed on any two members of the group to produce a third member) derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if youknow the original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse [8].

Understanding ECC needs full mathematical background on elliptic curves. Elliptic curves are not ellipses. The general cubic equation of elliptic curves is $y^2 + axy + by = x^3 + cx^2 + dx + e$. But for our purpose it is sufficient to limit the equation to the form $y^2 = x^3 + ax + b$.

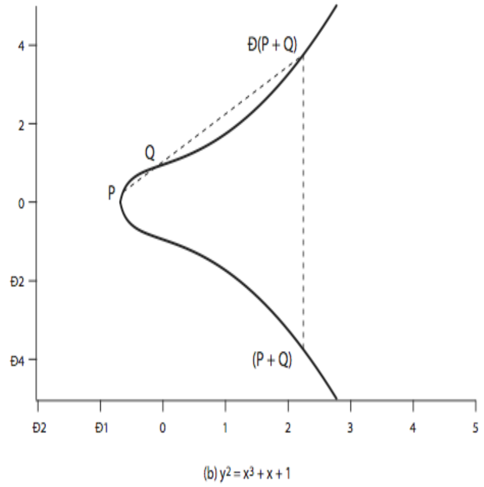

Figure 2: elliptic curve

A group can be defined based on the set E_P (a,b) for specific values of a and b[10]. If P,Q R are points on E_P (a,b) the relations commutativity, associativity, existence of an identity element and existence of inverse hold good[11]. The heart of ECC is discrete logarithm problem that can be stated as “it should be very hard to find a value k such that Q=Kp where P and Q are known’. But ‘it should be relatively easy to find Q where k and P are known’ P, Q are points on the elliptic curve [5][6].

Key Generation An elliptic curve public key is a point Q = dG which is a multiple of the generator G for $1 \leq d < n$. Poor randomness might manifest itself as repeated values of d, and thus repeated public keys observed in the wild. In contrast to RSA, where poor random number generators and bugs have resulted in distinct RSA moduli that can be factored using the greatest common divisor algorithm when they share exactly one prime factor in common, an elliptic curve public key appears to have no analogous property. We are unaware of any similar mathematical properties of the public keys alone that might result in complete compromise of the private keys, and they are unlikely to exist because discrete logarithms have strong hardcore properties [7, 12]. We checked for these problems by looking for collisions of elliptic curve points provided in public keys. In practice, however, it is not uncommon to encounter the same public key multiple times: individuals can use the same key for multiple transactions in Bit coin or the same key pair can be used to protect different servers owned by the same entity.

II. Related Work

Cryptography [9, 10, 11] is the art and science of achieving security by encoding messages to make them readable. The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence it is more vulnerable of duplicating of data and re-distributed by hackers. Therefore the information has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of wireless communication, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the wireless. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities.

Purpose of Cryptography
Cryptography serves following purposes:
Confidentiality: The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.

Authentication: Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

Integrity: The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Non- repudiation: Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.
Access Control: Access Control specifies and controls who can access what.

Availability: The principle of availability states that resources should be available to authorized parties all the times.

In this paper two different encryption schemes for database. Both schemes use RSA algorithm. The first one is field based encryption system. All fields are accessed by master key of user. Next, represents record oriented encryption. It uses only one master key. This method applied in subsets and integers group. [13-17, 20]To provide security to the database is one of the complicated problems. For this, asymmetric crypto system is commonly used. Basically encryption keys are used to write data in protected fields. Decryption keys are used to read the data. So it provides the access rights for user. The simpleencryption method for database is RSA method. RSA master key pair contains two different keys. Encryption keys are used to represents the right of write operation. The right of read operation is represents by decryption keys. The key pair is maintains by database manager. All rights of fields are combined by RSA master keys. Database manager establishes each field of database in database encryption schemes. Access rights are allocated by using this method. This is used to allocate the access rights depend upon the user requirements. Generally, dynamic data storage is used. Read operation is the most frequent compare to other. Generally, write operations remove to write proxy for approval [18-20]. This method prevents from the outside attack. It prevents the traffic analysis also. To manage key management problems, both schemes use the RSA master key. Both provide the access rights to user and database security.

Elliptic curve cryptography was introduced in the mid-1980s independently by Koblitz and Miller [22, 21] as a promising alternative for cryptographic protocols based on the discrete logarithm problem in the multiplicative group of a finite field (e.g., DiffieHellman key exchange [23, 21] or ElGamal encryption/signature [24, 21]). ECC is a kind of public key cryptosystem like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. The security level which is given by RSA, can be provided even by smaller keys of ECC. For example, the 1024 bit security strength of a RSA could be offered by 163 bit security strength of ECC.

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

III. METHODOLOGY

Proposed system focuses to reduce key size and increase the speed of cryptography algorithm. The key size is reduced simultaneously speed increased with same security level. Our proposed system to use Elliptical curve cryptography (ECC) is a public key encryption technique based on AEDA procedure. Abet Efficient Defended Algorithm is support of multimedia encryption method. Original text or image is transformed into pixel value and arranged in rows and columns pattern. After that the points are encrypted by AEDA method finally image and text converted into cipher text and image. The resulting system gives comparatively small block size, high speed and high security. . ECC can yield a level of security with a 256-bit key that RSA require a 3,072-bit key to achieve. Because ECC-AEDA helps to establish corresponding security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are plain to cipher. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email [25]. Encryption algorithms are classified into two groups: Symmetric-key (also called secret-key) and Asymmetric-key (also called public-key) encryption.

Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption [26].

Elliptic curve cryptography (ECC) is a modern type of public-key cryptography wherein the encryption key is made public, whereas the decryption key is kept private. This particular strategy uses the nature of elliptic curves to provide security for all manner of encrypted products [25].

Elliptic-Curve Abet Efficient Defended Algorithm (ECAEDA) is riddle key assertion tradition that grants two social events, each having an elliptic-curve public– private key match, to develop a common secret over a precarious channel. This shared riddle may be explicitly used as a key, or to deduce another key. The key, or the decided key, would then have the capacity to be used to scramble coming about trades using a symmetric-key figure. It is a variety of the AEDA tradition using elliptic-twist cryptography. AEDA algorithm is the process of point addition and multiplication.

Advantages Of ECAEDA Over RSA:
Complexity of the algorithm is reduced.
Computational speed increased.
Amount of encrypted data is smaller.
Key size is small.

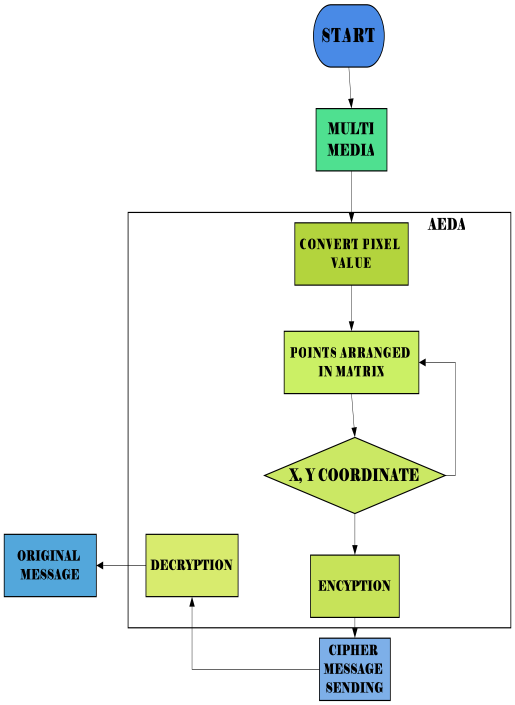

Figure 3. Flow Graph of proposed Algorithm

In figure 3 shows that the flow of encryption and decryption process. First we are take M×N binary multimedia as input X. Each pixel value of media data X, that is called message m, can be converted into the coordinate (X m, Y m) that are the point on elliptic curve. Where m is message K is the random positive integer. Encryption/decryption system require a point on G and an elliptic group E p(a, b). User A select a private key and generate a public key nA .G. To encrypt and send message pm to B, A choose a random positive integer k and produce the cipher text Cm consisting of the pair of points. Where PB is the public key of user B. Decrypt the cipher text using the method.

IV. PROPOSED ALGORITHM

A. Abet Efficient Defended Algorithm (AEDA)

```
1. Begin
2. int pixel; //multimedia is converted into pixel value
3. int group[pixel];
4. Pm=group [pixel]; // Group the pixels and convert to single large integer value for each group.
5. Pm= pointadd()    //Each pixel value of media X, that is called message m, can be converted into the coordinate (X m, Y m)
{
```

```
for i=0 to 255
for j=0 to pixel;
X[i][j]= Pixel x k + J; // Y[i][j]=$\sqrt{x^3 + ax + c}$
 J++;
End for
End for
}
6. for i=0 to 255  // Pair up the points 'Pm' which is the plain message input for the  Encryption system
7. for j=0 to pixel;
  Order the points;
End for
End for
Encryption:// Encryption/decryption system require a point on G and an elliptic group   E p(a, b).The sender chooses an arbitrary number $n_A$ between the range [1, n-1].
$n_A$ is the private key of the sender.
                 At that point the sender creates people in general key utilizing the equation
                        Sr = $n_A$ *G
8. for i=0 to 255
 for j=0 to pixel;
Pci[i]={kC, Pm+kSr }// sender chooses an arbitrary number k from [1,n-1]
 End for
End for
Pct={kC, M+kSr } // Encrypted text message
Decryption
9. Pm=Pci2-pointmul(int $n_B$, int Pci1); //Decryption multimedia values
M= Pct2-pointmul(int $n_B$ , int Pct1); //Decryption text message
Int pointmul(){
Z=$n_B$ *Pci1;
}
10. End
```

The process of AEDA provides high efficiency with small key size.ECC that be implemented on 160-bit nearly offer the same level of security in the resistance against compared with 1024-bit RSA attacks. That led to improved performance and better storage requirements [44, 45].

IV. Results and Discussion

A. KEY SIZE AND GENERATION TIME

In proposed system use elliptic curve cryptography instead of RSA algorithm because key size of ECAEDA is small compared to the RSA algorithm with same security level. The comparision of key size same security level shown in figure 6. Both AEDA and RSA algoritm systems the key generation times were not the same every time, even though the key length is the same and it can sometime a take very long time to generate the keys. Figure 7 shows that key generation time. ECAEDA have smaller key size so key generation time is reduced compared to RSA.

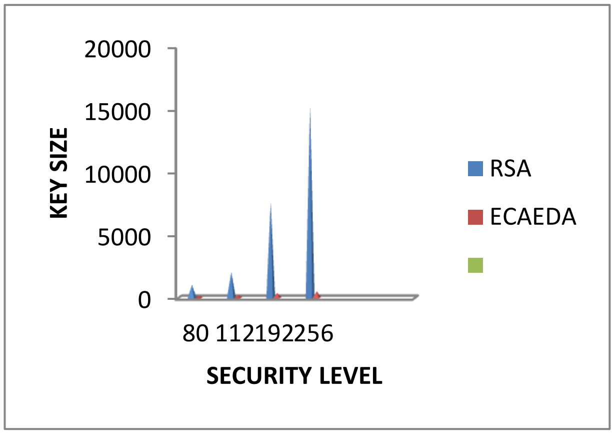

Figure 4: Comparison of Key size and Security level.

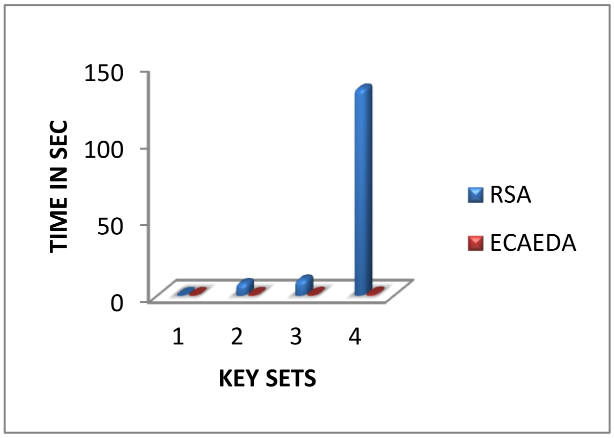

Figure 5:Key Generation Time

B. ENCRYPTION/DECRYPTION TIME

Figure 2 shows the Encryption times for ECC and RSA algorithms, smaller key sizes ECC provides much faster encryption/decryption as compared to RSA. Since RSA uses higher key sizes the encryption/decryption times grow up exponentially with the given key size.

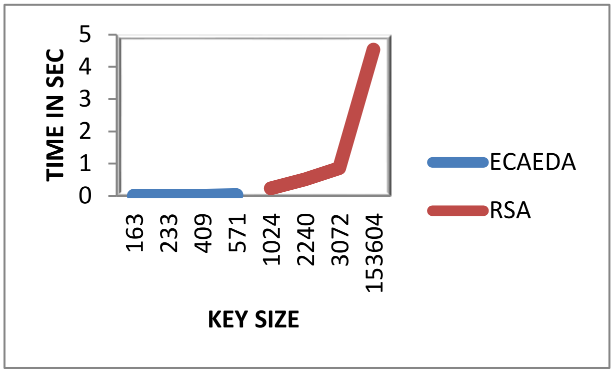

Figure 6: Comparison of Encryption Times

Figure 8 shows the decryption times. Based on the key size ECC decryption time varies linearly but RSA it increases exponentially due to the large amount of computation implicated as shown in the Figure 4. The decryption time is lesser than the encryption time both ECC and RSA algorithms.

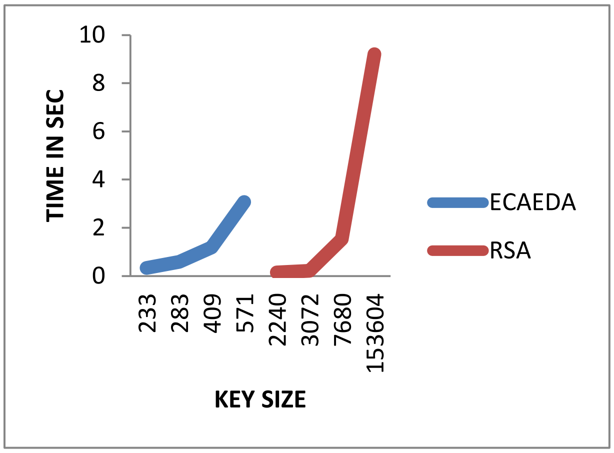

Figure 7: Comparison of decryption times

V. CONCLUSION AND FUTURE SCOPE

In proposed system algorithm implement elliptic curve cryptography instead of RSA algorithm. ECAEDA is a private key encryption algorithm with small key size but RSA have large key size. In proposed system achieve same security level with small key size compared to RSA algorithm. ECAEDA have small key size therefore key generation time reduced simultaneously encryption/ decryption computation time also reduced. Overall performance of ECAEDA increased. AEDA makes it an ideal choice for moveable, mobile and low power applications. Future work, to expand our algorithm set to include other elliptic-curve algorithms, different block ciphers, further reduce the key size and complexity.

REFERENCES

[1] Jasmin Syed, J S Ananda Kumar " Cryptography Algorithms For Providing Security To Data While Transferring Over Network" International Journal of Scientific & Engineering Research Volume 8, Issue 5, May-2017 ISSN 2229-5518

[2] William Stallings, "Cryptography and etwork Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.

[3] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 226-233, July 2012.

[4] Gurpreet Singh, Supriya " A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" international Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.

[5] William Stallings, Cryptography and Network Security, Principles and Practice. ed.,Prentice Hall, New Jersey,2003.

[6] Padma Bh, D.Chandravathi, P.Prapoorna Roja Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's MethodPadma Bh et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1904-1907

[7] R. Schoof. Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p. Mathematics of Computation, Vol. 44, No. 170, pp. 483-494, April 85.

[8] C. Nithiya, IIR. Sridevi ECC Algorithm & Security in CloudInternational Journal of Advanced Research in Computer Science & Technology (IJARCST 2016) Vol. 4, Issue 1 (Jan. - Mar. 2016)

[9] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.

[10] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education,2004.

[11] Mitali, Vijay Kumar and Arvind Sharma, "A Survey on Various Cryptography Techniques" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 4, July-August 2014

[12] Samta Gajbhiy e,Dr. Sanjeev Karmakar, D r. Monisha Sharma,Dr. Sanjay Sharma, Dr. M K Kowar, "Application of Elliptic Curve Method in Cryptography: A Literature Review", Samta Gajbhiye et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4499 - 4503

[13] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[14] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[15] Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[16] Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.

[17] Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.

[18] Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.

[19] Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.

[20] P.R.Hariharan & Dr. K.P. Thooyamani, " Various Schemes for Database Encryption - A Survey", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8763-8767.

[21] Sharad Kumar Verma and Dr. D.B. Ojha , A Discussion on Elliptic Curve Cryptography and Its Applications , IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012 ISSN (Online): 1694-0814

[22] Victor S. Miller. Use of elliptic curves in cryptography. In H.C. Williams, editor, Advances in Cryptology CRYPTO'85, vol. 218 of Lecture Notes in Computer Science, pp. 417-426. Springer-Verlag, 1986.

[23] Whitfield Diffie and Martin E. Hellman. New directions in cryptography, IEEE Transactions on Information Theory, 22(6):644-654, 1976.

[24] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4):469- 472, 1985.

[25] https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

[26] William Stallings, "Cryptography and network Security: Principles and Practice", Pearson Education/Prentice Hall, 5th Edition.