Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 85 (2015) 34666-34670

ISSN: 2229-712X

A survey of low power elliptic curve cryptography for smart network

K. Immanuvel Arokia James, A.Karthikeyan and M. J. Carmel Mary Belinda

Department of EEE VEL Tech Multi Tech Dr. RR Dr. SR Engg College, Chennai, India.

ARTICLE INFO

Article history:

Received: 19 May 2012;

Received in revised form:

22 August 2015;

Accepted: 29 August 2015;

Keywords

Wireless Network,

Elliptic curve Cryptography,

Sensor Network.

ABSTRACT

The proposed project is to implement a novel idea in Sensor networks. Normally Sensor networks are used to sense environment and collect data. Security in such networks is a big challenge. The first challenges of security in sensor networks lie in the conflicting interest between minimizing resource constraints and maximizing security. An implementation of operating system may reduce the risk level of handling secure data but sensor networks also introduce severe resource constraints due to their lack of data storage and power. Thus we employ a hardware cryptographic unit with low power consumption. The working memory of a sensor node is insufficient to even hold the variables (of sufficient length to ensure security) that are required in asymmetric cryptographic algorithms. A symmetrical key crypto security system will be less adequate to handle the modern secure threats, due to that a much complex asymmetric crypto system called elliptic curve cryptography is designed with various optimizing units(ex: pipeline, scheduling) to achieve greater security and to consume much power with reduced resources constraint.

© 2015 Elixir All rights reserved.

1. Introduction

A computer network, often simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information. Networks may be classified according to a wide variety of characteristics such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.

Wireless network:

Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using a transmission system called radio waves. This implementation takes place at the physical level (layer) of the network structure.

Sensor network:

Sensor Network is a global exchange for sensor information. It allows researchers and scientists to share data with authorized partners. Authorized users can manage sensor installations, visualize collected data and share it with trusted partners.

Wireless sensor network:

A WSN consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, enabling also to *control* the activity of the sensors. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, industrial process monitoring and control, machine health monitoring.

Communications systems play a pivotal role in the success of wireless sensor networks. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks. But sensor networks also introduce severe resource restraints due to lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. A number of independent nodes, communicating wirelessly over limited frequency and bandwidth constitutes a wireless sensor network. Unlike traditional networks, sensor networks depend on dense deployment and coordination to execute their tasks. A wireless sensor network is a special network which has many constraints comparing to the traditional computer network. Due to these constraints it is difficult to directly employ the security approaches to the area of wireless sensor networks. A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

.Problems In Sensor Security

Some problems and limitations of sensor security are outlined as below.

(i) Limited Resources:

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

(ii) Limited Memory and Storage Space:

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. . For example, one common sensor type has an 8-bit, 4MHZ CPU only with only 8K (total) of memory and disk space. With such a limitation, the software built for the sensor must also be quite small. The total available code space

Tele:

E-mail addresses: immanuel_james@yahoo.com

© 2015 Elixir All rights reserved

of Tiny OS, the de-facto operating system for wireless sensors, is just about 4K, and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

(iii) Power Limitation:

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the life span of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions. (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

In order to implement security mechanism in sensor networks, we need to ensure that communication overhead is less and consumes less computation power. Sensor networks are vulnerable to a variety of security threats such as DoS, eavesdropping, message replay, message modification, malicious code, etc. In order to secure sensor networks against these attacks, we need to implement message confidentiality, authentication, message integrity, intrusion detection and some other security mechanism. In order to have more secure data transaction between nodes in wireless sensor network cryptography techniques are widely used.

2. Cryptography

The word cryptography in Greek means "secret writing." The term today refers to the science and art of transforming messages to make them secure and immune to attacks.

Cryptography allows secure transmission of private information over insecure channels (for example packet-switched networks).Cryptography also allows secure storage of sensitive data on any computer. Cryptography is the practice and study of hiding information.

- Cryptography guarantees basic security services authorization, authentication, integrity, confidentiality, and non-repudiation in all communications and data exchanges in the new information society.
- These guarantees are achieved as follows:

– Confidentiality - through encryption

– Authentication - through digital signatures and digital certificates

Integrity - through generating a digital signature with a public key and obtain the message digest. Then hashing the message to obtain a second digest. If the digests are identical, the message is authentic and the signer's identity is proven.

Non-repudiation - through digital signatures of a hashed message then encrypting the result with the private key of the sender, thus binding the digital signature to the message being sent

Non-replay – through encryption, hashing, and digital signature

In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

Sensor Network Communication

In existing system, an asymmetric RSA algorithm can be implemented for sensor in an efficient manner by using optimized computation. We have simulated the protocol in NS2.34 platform. The energy requirement gives an optimistic result quite similar to symmetric protocol energy requirement for sensor.

In existing system has three steps for the energy consumption of RSA security protocol.

- Design a model for secured data communication from cluster node to cluster head.
- We have use the RSA algorithm to reduce the computation cost and
- We have changed the packet format.

Modification of Packet Format

We change the packet format of the message by adding an extra field called the identification field. The packet formats of the original, modified and encrypted are shown in Figure 1, Figure 2, and Figure 3 respectively.

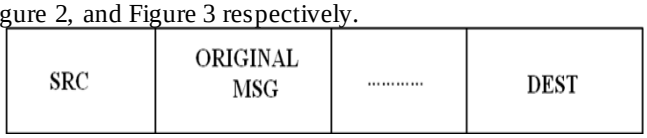

Figure1. Original message packet format

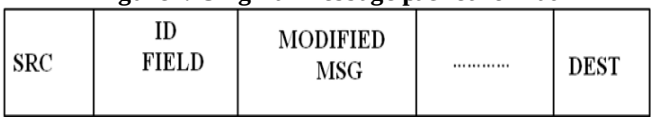

Figure2. Modified Message Packet Format

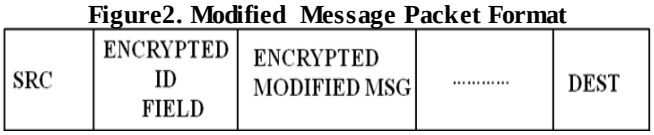

Figure 3. Encrypted Message Packet Format

Elliptic Curve Cryptography

ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements.

For current cryptographic purposes, an *elliptic curve* is a plane curve which consists of the points satisfying the equation

$$y^2 = x^3 + ax + b,$$

(iv) Along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.) This set together with the group operation of the elliptic group theory form an Abelian

group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

ECC mathematical derivation

A non-super singular elliptic curve E over binary fields $GF(2^m)$ is defined to be the set of solutions.

(x,y) E $GF(2^m)$ x $GF(2^m)$ to the equation

$y^2 + xy = x^3 + ax^2 + b$…… (1)

where a,b € $GF(2^m)$,b ≠ 0, together with the point O at infinity. E forms a commutative finite group by the well-known law of chord and tangent, with O being the group identity.

Let P € E(K) and k€ N, the equation (2) is used to compute the new point

Q=kP =f + P + P +...+P,……..(2)

Q is called ECMLT. *Q* is another point on the curve E. The binary representation of the random integer *k* has m bits, where *k*, €{O, I} .

ECC sensor network

In proposed system, asymmetric ECC algorithm can be implemented for sensor in an efficient manner by using optimized computation. We will be simulating the protocol in NS2.34 platform. In this model we designed the same cluster based communication model. We have taken initial power, transmission and receiving range is same for the entire cluster node and the cluster head as well. When the sensor nodes are deployed, they make a cluster within their range. Each cluster has a cluster head and other node in the cluster is called cluster node. It is the duties of these cluster head to communicate with the base station of the network.

Each cluster head generates a public key suite and a private key suite dare based on elliptic curve parameter selections and algorithms. Whenever cluster node generates a new private key suite and public key suite, it broadcasts the private key to the base station encrypted with the base station public key. At the same time it will broadcast its public key to its cluster node.

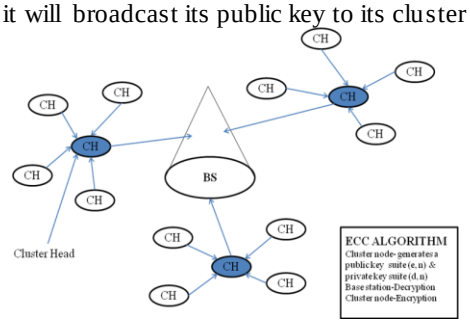

Figure 4. ECC Cluster-Based Sensor Network

Again for security purpose the base station re-generates the private and public key and broadcasts its public key encrypted by each public key of the cluster head. Hence only the cluster heads of the network access the public key of the base station and a secure communication between the base station and the cluster head is preserved. The frequencies of broadcasting the public keys are different for base station and for the cluster head. As the base station has no energy and memory constrain problem, its broadcasting frequency of the public key is more than the cluster head's public key broadcasting.

Proposed system block diagram

ECC parameter selection can select the points from the elliptic curve projective co-ordinates. To ECC all parties must agree on all the elements defining the elliptic curve, that is, the *domain parameters* of the scheme. The field is defined by *p* in the prime case and the pair of *m* and *f* in the binary case. The elliptic curve is defined by the constants *a* and *b* used in its defining equation. Finally, the cyclic subgroup is defined by its *generator G*. A key pair *x* and *y* is generated for a set of domain parameters (*p, q, g* {*domain_parameter_seed, counter*}).

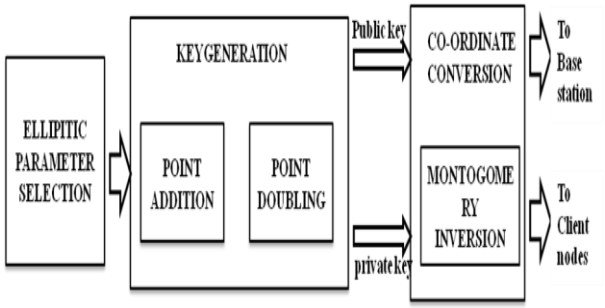

Figure 5. ECC key generations

The key generation process involves two major operations,

a)Point addition (ECADD)

b) Point doubling (ECDBL)

These operations are done by an elliptic curve processor.

An elliptic curve processor

An ECC processor consists of a main control block, an ECC block and finite field block. An ECC block for arithmetic operations involves point addition and point doubling. Finite field block perform the inversion, addition, multiplication and square operations. ECC block and finite field block are controlled by main control block.

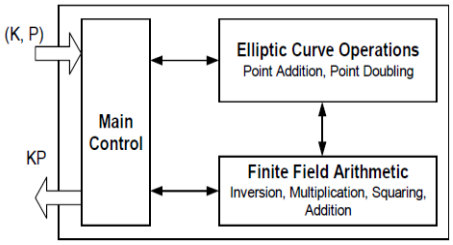

Figure 6. An elliptic curve processor

Point addition (ECADD)

Point addition is defined as taking two points along a curve *E* and computing where a line through them intersects the curve. We use the negative of the intersection point as the result of the addition. It is the addition of two points J and K on an elliptic curve to obtain another point L on the same elliptic curve. Consider two distinct points J and K such that J = (xJ, yJ) and

K = (xK, yK)., Let L = J + K where L = (xL, yL), then xL = s2 - xJ – xK mod p

yL = -yJ + s (xJ – xL) mod p

s = (yJ – yK)/(xJ – xK) mod , s is the slope of the line through J and K.

If K = -J i.e. K = (xJ, -yJ mod p) then J + K = O. where O is the point at infinity.

If K = J then J + K = 2J then point doubling equations are used.

Also J + K = K + J

Geometrical Explanation

Consider two points J and K on an elliptic curve as shown in figure (a). If K ≠ -J then a line drawn through the points J and K will intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respect to x-axis gives the point L, which is the result of addition of points J and K. Thus on an elliptic curve L = J + K. If K = -J the line through this point intersect at a point at infinity O. Hence J + (-J) = O.This is shown in figure (b). O is the additive identity of the elliptic curve group. A negative of a point is the reflection of that point with respect to x-axis

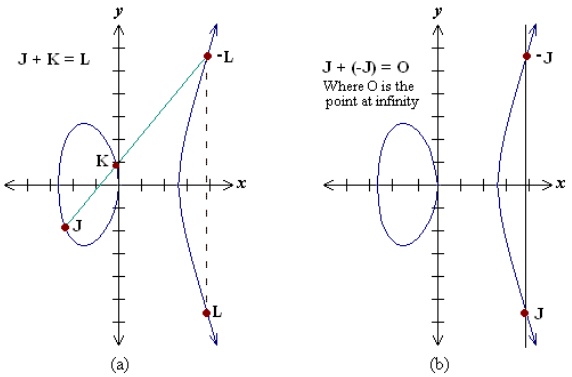

Figure 7. Geometrical representation of elliptic point addition

Analytical Explanation

Consider two distinct points J and K such that J = (xJ, yJ) and K = (xK, yK)

Let L = J + K where L = (xL, yL), then

$xL = s2 - xJ - xK$

$yL = -yJ + s(xJ - xL)$

$s = (yJ - yK)/(xJ - xK)$, s is the slope of the line through J and K.

If K = -J i.e. K = (xJ, -yJ) then J + K = O. where O is the point at infinity.

If K = J then J + K = 2J then point doubling equations are used. Also J + K = K + J.

Point Doubling (Ecdbl)

Point doubling is the addition of a point J on the elliptic curve to itself to obtain another point L on the same elliptic curve. Like point addition except we take the tangent of a single point and find the intersection with the tangent line.

Consider a point J such that J = (xJ, yJ), where $yJ \neq 0$

Let L = 2J where L = (xL, yL), Then

$xL = s2 - 2xJ \mod p$

$yL = -yJ + s(xJ - xL) \mod p$

$s = (3xJ$

$2 + a) / (2yJ) \mod p$, s is the tangent at point J and a is one of the parameters chosen with the elliptic curve

If yJ = 0 then 2J = O, where O is the point at infinity.

Geometrical explanation

To double a point J to get L, i.e. to find L = 2J, consider a point J on an elliptic curve as shown in figure (a).

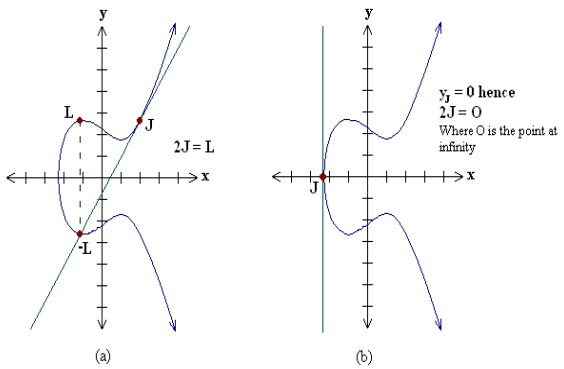

Figure 8. Geometrical representation of elliptic point doubling

If y coordinate of the point J is not zero then the tangent line at J will intersect the elliptic curve at exactly one more point –L. The reflection of the point –L with respect to x-axis gives the point L, which is the result of doubling the point J.Thus L = 2J.

If y coordinate of the point J is zero then the tangent at this point intersects at a point at infinity O. Hence 2J = O when yJ = 0. This is shown in figure (b).

Analytical Explanation

Consider a point J such that J = (xJ, yJ), where $yJ \neq 0$

Let L = 2J where L = (xL, yL), Then

$xL = s2 - 2xJ$

$yL = -yJ + s(xJ - xL)$

$s = (3xJ$

$2 + a) / (2yJ)$, s is the tangent at point J and a is one of the parameters chosen with the elliptic curve

If yJ = 0 then 2J = O, where O is the point at infinity.

Block Diagram Explanation

ECC is based on the additive group of points on an elliptic curve over a FE It derives its security from the hardness of the elliptic curve discrete logarithm problem. ECC is one of the best schemes in public key cryptosystems, and it has smaller key size. ECMLT is the most expensive operation in ECC related algorithms. One way to compute ECMLT is to do point addition (ECADD) and doubling (ECDBL) loop operations over elliptic curve. Both ECADD and ECDBL operations composed of FF operations, such as addition, square, multiplication and inversion. These FF operations are divided into groups which are used at different stage to archive pseudo-pipelined ECMLT.

Proposed System Modules

1. Network Design
2. ECC Key generation

a. Point addition

b. point doubling

c. mont inversion

d. pipeline scheduling

3. Encryption
4. Decryption

Proposing Methodology

ECC Design

Usually two independent ECMLTs are computed in the elliptic encryption algorithms. The ECMLT architecture with uniform addressing plays an important role in elliptic encryption algorithms shown in Fig.

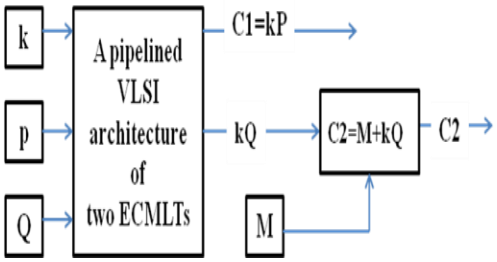

Figure 9. System diagram of ECC algorithm

Elliptic curve families:

Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field.Two families of elliptic curves are used in cryptographic applications.

1. Prime curve over Z_p
2. Binary curve defined over $GF(2^m)$

Prime Curve Over Z_p

We use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through p-1 and in which calculations are performed modulo p.Prime curves are best for software applications, because the extended bit-fiddling operations needed by binary curves are not required.

Binary Curve Defined Over Gf(2^m)

For a binary curve defined over GF(2^m),the variables and coefficients all tak on values in GF(2^n)and in calculations are performed over GF(2^n).The binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful ,fast cryptosystem.

Elliptic Curve Algorithms

- Elliptic Curve Digital Signature Algorithm (ECDSA),
- Elliptic Curve Diffie-Hellman Key exchange(ECDH),
- Elliptic Curve multiplication algorithm (ECMLT).

Conclusion

In this project, an enhanced asymmetric cryptography technique is proposed to reduce the key length, power consumption and improve security. In addition, the ECDCA was used to provide the authentication to the receiver. Asymmetric cryptography provides two different key for more secure communication than symmetric key. ECC key generation process involves various operation like point addition, point doubling, point multiplication using this operation public key and private key are generated. These keys are used to encrypt and decrypt the message in secure manner. This can be simulated in model sim 6.3f and synthesis by using quatars II and implemented in cyclone 3FPGA.

REFERENCES

[1] Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede L. Buttyan, V. Gligor, and D. Westhoff (Eds.): ESAS 2006, LNCS 4357, pp. 6–17, 2006. c_Springer - Verlag Berlin Heidelberg 2006.

[2] Very low-power flexible GF(p) elliptic-curve crypto-processor for non-time-critical applications Ahmadi, H.R.; Afzali-Kusha, A.; Sch. of Electr. & Comput. Eng., Univ. of Tehran, Tehran, Iran. Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on 24-27 May 2009 page(s): 904 - 907

[3] J.S. Bridle, "Probabilistic Interpretation of Feedforward Classification Network Outputs, with Relationships to Statistical Pattern Recognition," *Neurocomputing—Algorithms, Architectures and Applications*, F. Fogelman-Soulie and J. Herault, eds., NATO ASI Series F68, Berlin: Springer-Verlag, pp. 227-236, 1989. (Book style with paper title and editor)

[4] W.-K. Chen, *Linear Networks and Systems*. Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

[5] H. Poor, "A Hypertext History of Multiuser Dimensions," *MUD History,* http://www.ccs.neu.edu/home/pb/mud-history.html. 1986. (URL link *include year)

[6] K. Elissa, "An Overview of Decision Theory," unpublished. (Unplublished manuscript)

[7] R. Nicole, "The Last Word on Decision Theory," *J. Computer Vision,* submitted for publication. (Pending publication)

[8] C. J. Kaufman, Rocky Mountain Research Laboratories, Boulder, Colo., personal communication, 1992. (Personal communication)

[9] D.S. Coming and O.G. Staadt, "Velocity-Aligned Discrete Oriented Polytopes for Dynamic Collision Detection," *IEEE Trans. Visualization and Computer Graphics*, vol. 14, no. 1, pp. 1-12, Jan/Feb 2008, doi:10.1109/TVCG.2007.70405. (IEEE Transactions).

Authors:

K. IMMANUVEL AROKIA JAMES is pursuing PhD in VEL TECH Dr. RR & Dr. SR Technical University, Chennai, India. He is currently working as Assistant Professor cum Head of the Department of EEE at VEL Tech Multi Tech Dr. RR Dr. SR Engineering College.

Email: immanuel_james@yahoo.com

A. KARTHIKEYAN is pursuing PhD in ANNA University, Chennai, India. He is currently working as Assistant Professor in Department of EEE at VEL Tech Multi Tech Dr. RR Dr. SR Engineering College.

Email: a.karthik1982@gmail.com.

M. J. CARMEL MARY BELINDA is pursuing PhD in VEL TECH Dr. RR & Dr. SR Technical University, Chennai, India. She is currently working as Assistant Professor in Department of CSE at VEL Tech Multi Tech Dr. RR Dr. SR Engineering College.

Email: carmelbelinda@gmail.com