International Journal of

Emerging Research in Management &Technology

Research Article

May 2014

Public Key Encryption with Certifiable farm out Decryption

Mr. Obbu Sekhar.O [1], Mr. Siva Kumar.B [2], Mr. Anandan D [3], Mr. Venkatesan S [4]

[1] PG Scholar, [2] Assistant Professor[3] Assistant Professor [4] Assistant Professor

[1,2,3,4] Vel Tech Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai, India

Abstract—

This paper presents a cloud computing is an emergent technology for the data storage the user can store and share the documents using the cloud storage .To provide the data privacy various encryption standard are used the attribute based encryption is one of the type in data encryption standard the encryption is performed based on the user attributes .The cipher text is directly proportional to the number of attributes of the user in attribute based encryption the user who holds certain attributes can only decrypt the corresponding cipher text .The user who does not hold the attributes cannot able to decrypt the cipher text .One of the drawback of that attribute based encryption system is the cipher text size is increases when attributes are increases and same time decryption time also increases. To overcome this problem a proxy server perform decryption over cipher text to reduce the cipher text size then the server outsources the cipher text then the user decrypt the small size of cipher text to get the original content We cannot say that the decryption performance by the proxy server is correct so to verify the decryption perform whether correct or wrong the proposed system introduces a outsourced decryption with verification so the proposed system let the user to check whether the decryption performed on the proxy server is right or wrong..

Keywords – Attribute based encryption, outsourced decryption, certifiable.

I. INTRODUCTION :

In cryptography, there are two different types of methods to provide the security to a data. They are

1. Symmetric
2. Asymmetric.

Symmetric means same key for sender as well as receiver. Generally, cryptography concepts having three important blocks, they are Encryption, Key generation and Decryption.

Data transmission can be starts from sender who can only able to mix the original data with Key which is called as “Cipher Text”. Cipher Text Transmission process can be done through the network medium. Finally, cipher text can be received by receiver who knows the methodology done by the sender. Plain Text can be received without any attacks. Process can be shown in following figure 1.

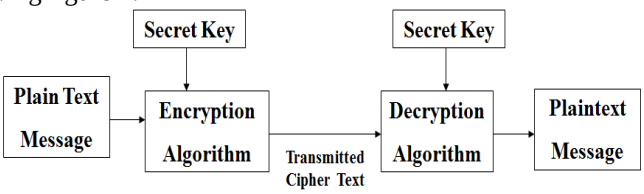


Figure 1: Block Diagram of Symmetric Encryption Process

Here in this process, the cryptanalysis can provides a systematic procedure which is called as “Cryptography Algorithms”. There are so many no. of cryptography algorithms like DES, Simplified DES, Double DES, Triple DES, IDEA, RC5 and Blowfish. Except RC5 remaining all algorithms having some standards (that means restrictions).

Suppose take DES and it’s all following generations are used for limited data i.e., all list of parameters are restricted up to its standard. IDEA (International Data Encryption Algorithm) which is having 64-bit input plain text and cipher text as a output using 128-bit Key size.

To overcome problems, this paper introducing ABE encryption algorithm. This contains user attributes based on that the plain text is converted into cipher texts using (ABE). It can be used for also provide the security analysis of Hand-Held Devices like Mobiles, Laptops, PDA’s etc.

A Principles Of Public Key Cryptosystem:

The concept of public-key cryptography evolved from an attempt to attack two of the most difficult problems associated with symmetric encryption. The first problem is that of key distribution, , key distribution under symmetric encryption requires either (1) that two communicants already share a key, which somehow has been distributed to them; or (2) the use of a key distribution center. Whitfield Diffie, one of the discoverers of public-key encryption (along with Martin Hellman, both at Stanford University at the time), reasoned that this second requirement negated the very essence of cryptography: the ability to maintain total secrecy over your own communication. As Diffie put it [DIFF88], “what good would it do after all to develop impenetrable cryptosystems, if their users were forced to share their keys with a KDC that could be compromised by either burglary or subpoena?”

The second problem that Diffie pondered, and one that was apparently unrelated to the first, was that of digital signatures. If the use of cryptography was to become widespread, not just in military situations but for commercial and private purposes, then electronic messages and documents would need the equivalent of signatures used in paper documents. That is, could a method be devised that would stipulate, to the satisfaction of all parties, that a digital message had been sent by a particular person? This is a somewhat broader requirement than that of authentication.

Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA). Grade information should only be available to students, their parents, and employees that require the information to do their job. Student enrollment information may have a moderate confidentiality rating. While still covered by FERPA, this information is seen by more people on a daily basis, I less likely to be targeted than grade information, and results in less damage if disclosed. Directory information, such as lists of students or faculty or departmental lists, may be assigned a low confidentiality rating or indeed no rating. This information is typically freely available to the public and published on a school's Web site.

B Advantages Of Cryptography:

The main advantage of the cryptography to provide a security a security over a transmission of data with the help of encryption algorithms and keys are used to convert the data in unreadable format.

It is a easy method to encrypt the data if any attacker attack the data he won't modified the data because it is encrypted with the help of public key cryptography.

C Objective:

In recent years to provide a security for a data transmission between Sender and receiver with the help of the public key cryptosystem using RSA algorithm .In ABE(attribute based encryption) is a new public key based one to many encryption that allows user to encrypt and decrypt data based on the user attribute .ABE is flexiable that enables access control over encrypt data stored in the cloud using some access polices and ascribed attribute private keys and cipher text. Previously ABE cipher text is first convert into a simple chipper text by using the proxy server and then user decrypt data but In these paper the cipher text is convert in to plain text with help of proxy and operated by the cloud .It overcome the decryption time for the user using ABE algorithm.

D Methodology:

The methodology behind the implementation of the ABE with verifiable outsource decryption because user collect the cipher text based on user attributes from the cloud .The decryption process will take the proxy server it is created by the user to operate on the cloud. It consumes less time for decryption and encrypted huge amount of data in the form text (bits).

E Overview of The Project:

We implemented ABE with verifiable decryption is mainly focus on CP-ABE system. It is a new public key based one too many encryption that is single sender can encrypt the multiple data for the same key(master key) each and every file contains a new key that is used to decrypt the data.

The encrypted data is stored in the cloud using some access polices and ascribed attributes user satisfied attribute then only user takes cipher text with transformation key from the cloud and it is send to the proxy server that contains a decryption algorithm it take input as the cipher text , transformation key . It produces output is plain text and send to the user. Here the private keys are the attributes the files are created with the help of the AND OR gates.

II. EXISTING SECURITY SYSTEM

Green *et al.* proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes or access policy into a simple ciphertext, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text.

Consider a cloud based electronic medical record system in which patients' medical records are protected using ABE schemes with outsourced decryption and are stored in the cloud. In order to efficiently access patients' medical records on her mobile phone, a doctor generates and delegates a transformation key to a proxy in the cloud for outsourced decryption; Given a transformed ciphertext from the proxy, the doctor can read a patient's medical record by just performing a simple step of computation. If no verification of the correctness of the transformation is guaranteed, however, the system might run into the following two problems: 1) for the purpose of saving computing cost, the proxy could return a medical record transformed previously for the same doctor; 2) due to system malfunction or malicious attack, the proxy could send the medical record of another patient or a file of the correct form but carrying wrong information. The consequence of treating the patient based on incorrect information could be very serious or even catastrophic.

A Disadvantages Of Existing System:

One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to pairing operations, and the number of pairing operations required to decrypt a ciphertext

grows with the complexity of the access policy. At the cost of security, only proven in a weak model (i.e., selective security), there exist several expressive ABE schemes where the decryption algorithm only requires a constant number of pairing computations.

III. PROPOSING SECURITY SYSTEM

In this paper, we first modify the original model of ABE with outsourced decryption in existing system to allow for verifiability of the transformations. After describing the formal definition of verifiability, we propose a new ABE model and based on this new model construct a concrete ABE scheme with verifiable outsourced decryption. Our scheme does not rely on random oracles.

A Advantages Of Proposed System:

- ✓ Proposed scheme does not rely on random oracles
- ✓ The scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.
- ✓ In these paper user provides proxy server that allow private key to translate any ABE cipher text into plaintext based on the user attribute .To provide a security of the data as well as it is easy to encrypt and decrypt the data.

  This project have been implemented in a java and text data is encrypt as well as decrypt based on the user attribute with the help of the private keys.

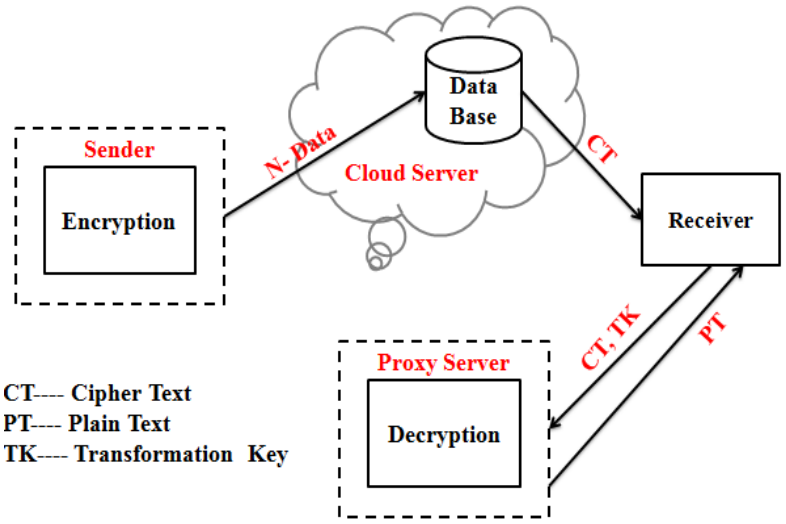
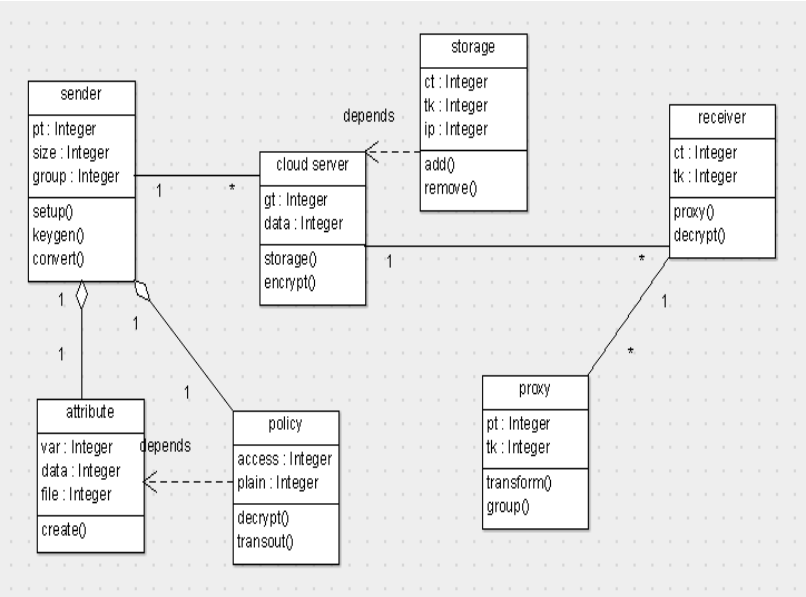


Figure 2: Proposed System Architecture.



Figue 3: Class Diagram

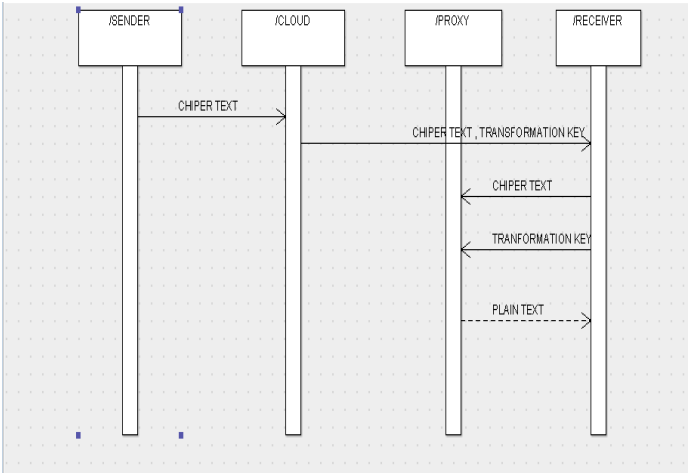


Figure 4: Sequence Diagram

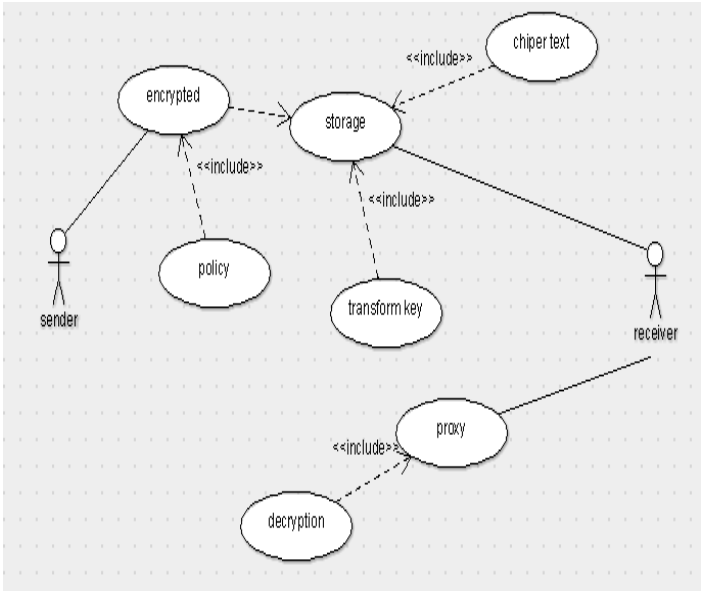


Figure 5: Use Case Diagram

IV MODULE DESCRIPTION

A Setup Unit:

The setup algorithm is used to take input of two parameter that consists of size of the group and universal descriptor .The group size is used the group of a prime order p for each and every attribute we need to calculate the public key that contain different parameters to provide a more security of the data .The output of the algorithm is the public key which is used to encrypt the data from the user side.

A.1 Definition of a Bilinear Map:

Let be G an algorithm that takes as input a security parameter λ and outputs a tuple (p,G,Gt,e) where G and Gt are the multiplicative cyclic group of p and e : G1XG2 → G3 is a map such that

1) **Bilinearity:** $e(u^a,v^b) = e(u,v)^{ab}$ for all and (g , h) ϵ G and a , b ϵ zp*
2) **Nondegeneracy:** e(g,h)=z2) **Nondegeneracy:** e(g,h) ≠ 1 whenever .(g , h) ≠ Ig
3) **Computable:** An efficient computability for any input pair. We refer to the tuple (p,G,Gt,e) as a bilinear group.

The setup algorithm working procedure can be explained below in the following steps

Setup(λ,U)

1. This algorithm take input as two parameters λ,U
   Where
   λ is size of the group
   U is universal description
2. It first run g(λ) to obtain (p,G,Gt,e)
3. Where G and Gt are the cyclic group of prime order p.

4. It choose g,u,v,d ϵ G
   a. α,α ϵ Zp* uniformly at Raandom
5. For each attribute i ϵ U it choose a random value si ϵ Zp*
6. Pk = (G,Gt,e,g,u,v,d, g^{α} ,e(g,g),Ti=$g^{s(i)}$)
7. Msk= α

B Key Generation unit:

The key generation algorithm is randomely picks the value of t ϵ zp* the secret key sks = (S,k,K0,K1,Kt) is computed as the k= g^{α} $g^{\alpha t}$ K0= g^{1} ,Kt= T^{i} for all ϵ S.

In these algorithm user has to calculate the private key for decrypt the data with the help of the key generation it takes input as a message that contains the data int the form of binary digit formate using ABE encryption it convert the cipher text.

C Encryption & Storage Unit:

The mysql is used to store the data in the form table that contain the rows and columns formate that act the back end of the project .these mysql is connected to the any programming language with of the syntax as well as the commands .

MySQL databases consist of a(ny) number of tables. Tables hold the data. Tables are made up of columns and rows. A user that has been given CREATE and DROP permissions on a database can create and remove tables of that database. The CREATE TABLE command simultaneously creates the table and defines its structure (although the structure of the table can later be changed using the ALTER TABLE command).

How it works for encryption :

1. List of users U = {u1; u2,….. un)
2. List of Attributes A = {a1; a2; , , , , ak)
3. Each user will be assigned a subset of attributes
4. D = {d1; d2,,,,, dx0 Where D ϵ A
5. Each encrypted _le will be assigned an access tree T in which:
6. Leaf Nodes are attributes in A.
7. Each none leaf node is a gate Node with assigned
8. Threshold.
9. The threshold kx ,0 < kx < numx where numx is the number of children for node x.
10. If the Node is an AND kx = numx.
11. If the Node is an OR kx = 1

How it works with Example:

a. Attributes: { Doctor ; Nurse ; A ;B ; C }.
b. Users:
   1. User1: { Doctor ; A }
   2. User2: { Doctor ; C }:
   3. User3: { Nurse ; B }
c. Access Tree:

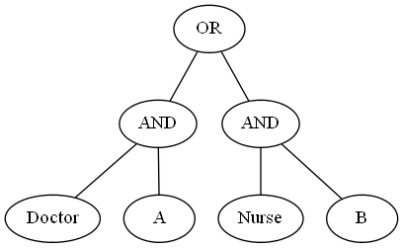


Figure 6: Searching Technique

The encryption algorithm take the input public key parameters pk and a message M is used to encrypted the data with the help of the LSSS structure A=(a,p) where A is L*N matrix and p is the row of the each attribute it choose a random vector of the two values provided by the access structure and finally the original plain text is converted in to the cipher text it can be achieve the security of the data.

D Decryption Unit:

The decryption algorithm takes the input parameters of the public key parameters Pk , and private Sks=(S,K0,K1,Kt) for a set of attribute S and a cipher text CT=((A,P),C,C1,C1,C1… D1,C2,C2,C2..D2 i) for an access structure A=(A,P) if S does not satisfied the structure of the A it output is does not satisfied . suppose that S is satisified the access structure of the L=(1,2,3…….l) be defined as l={I; p(i) ϵ S }.

$$C1 . \frac{\prod_{i \epsilon I}(e(C1,i,K0).e(Kp(i),D1,i)^{\omega i})}{e(C'1,K)}$$

$$=M.\ e(g,g)^{\alpha s}.\frac{(\prod_{i\epsilon I} e(g,g)^{\alpha t A i.v.\omega i}}{(e(g,g)^{\alpha s}\, e(g,g)^{\alpha t s}} = M,$$

$$C2\ .\ \frac{\prod_{i\epsilon I}(e(C2,i,K0).e(Kp(i),D2,i)^{\omega i})}{e(C'2,K)}$$

$$=M.\ e(g,g)^{\alpha s'}.\frac{(\prod_{i\epsilon I} e(g,g)^{\alpha t A i.v.\omega i}}{(e(g,g)^{\alpha s'}\, e(g,g)^{\alpha t s}} = \tilde{M}$$

Obviously, the above CP-ABE scheme satisfies correctness. Observe that, in our construction, a cipher text includes three parts: (C1,C1,C1,D1) (c2,c2,c2, d2) and . The first and second parts are encryptions of message and a random message respectively, using the encryption algorithm of Waters' CP-ABE scheme . In fact, the second and third parts are redundant. However, the redundant parts are the point that we can construct a CP-ABE with verifiable outsourced decryption from the above CP-ABE scheme.

E Proxy Server Unit:

In computer networks a proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems Today, most proxies are web proxies, facilitating access to content on the World Wide Web.

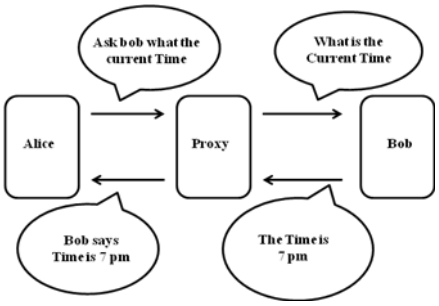


Figure 7: Model Data Retrive Technique

In the above example there are two user ane user is define as the alice and another user is defined as bod. Suppose alice send the information is encrypted with the bob public key and send to the proxy server it is an intermediate server transfer of data to the bob . bob can decrypt the data with the help of the private key of the allice Transferring of data between two computer devices.

V CONCLUSION

In this paper, we considered a new requirement of ABE with outsourced decryption: verifiability. We modified the original model of ABE with outsourced decryption proposed by Green *et al.*to include verifiability. We also proposed a concrete ABE scheme with verifiable outsourced decryption and proved that it is secure and verifiable. Our scheme does not rely on random oracles. To assess the practicability of our scheme, we implemented it and conducted experiments in a simulated outsourcing environment. As expected, the scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts

VI. WORK DONE AND DISCUSSION:

This paper presents a security of the data stored in the cloud and it is easily can decrypt the data based on the user attributes. The data is decrypted by the proxy server which is operated by the cloud .

REFERENCES:

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc. EUROCRYPT, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryp-tion for fine-grained access control of encrypted data," inProc. ACM Conf. Computer and Communications Security, 2006, pp. 89–98.

[3] R.Ostrovsky,A.Sahai,and B.Waters,"Attribute-basedencryption with non-monotonic access structures," inProc. ACM Conf. Computer and Communications Security, 2007, pp. 195–203. B. Waters, "Ciphertext-policy attribute-based encryption: An expres-sive, efficient, and provably secure realization," inProc. Public Key Cryptography, 2011, pp. 53–70.

[4] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," inProc. EUROCRYPT, 2010, pp. 62–91.

[5] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," inProc. CRYPTO, 2010, pp. 191–208.

[6] A. B. Lewko and B. Waters, "Unbounded HIBE and attribute-based encryption," inProc. EUROCRYPT, 2011, pp. 547–567.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," inProc. IEEE Symp. Security and Privacy, 2007, pp. 321–334.

[8] L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE," inProc. ACM Conf. Computer and Communications Security, 2007, pp. 456–465.

[9] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts,"Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.

[10] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," inProc. Public Key Cryptography, 2013, pp. 162–179.

[11] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," inProc. USENIX Security Symp., San Francisco, CA,USA,2011.

[12] M. Bellare and P. Rogaway, "Random oracles are practical: A para-digm for designing efficient protocols," inProc. ACM Conf. Computer and Communications Security, 1993, pp. 62–73.

[13] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle method-ology, revisited (preliminary version)," in Proc. STOC, 1998, pp. 209–218.

[14] J. B. Nielsen, "Separating randomoracle proofs from complexity theo-retic proofs: The non committing encryption case," inProc. CRYPTO, 2002, pp. 111–126.

AUTHORS:

1. Obbu Sekhar O, PG Scholar in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.
2. Siva Kumar B, Asst. Prof in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.
3. Anandan D, Asst. Prof in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.
4. Venkatesan S, Asst. Prof in VELTECH Multi Tech Dr.Rangarajan Dr. Sakunthala College of Engineering, Chennai.