International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-1 Issue-14 March-2014

Ciphertext Policy Attribute Set Based Encryption with One-Fold Data Access in Cloud

Surya Prabha.U.S[1], Marikkannu.P[2], Arul Vineeth.A.D[3]

Abstract

Cloud Computing is the most powerful paradigm in IT industry. Cloud users confide their valuable data's in cloud. The major concern in cloud computing is the privacy of outsourced data's. Several access control method has been employed to secure the outsourced data's. Hierarchical Attribute Set Based Encryption (HASBE) extends Ciphertext Attribute Set Based Encryption (CP-ASBE) method with a hierarchical user structure to attain scalability, flexibility and fine grained access control of user's data. Service provider has rampant storage capacity and computational power. But, it does not support constraint based verification system i.e. authorized user can access the data without any constraint. The proposed work provides high level of security for user data. Data is encrypted and managed by data owner which eliminates data replication in cloud environment. Here data consumer access resources directly from data owners. Attribute Authority plays the role of cloud service provider, trusted authority and domain authority. Attribute authority verifies the level of the data consumer and provides a packet with the level and key structure encrypted by notification key. Thus data consumer liaisons data owner with necessary information and obtain the data directly from the data owner.The proposed work is more secure and an effective way to access data in cloud environment without data replication. Also computation cost is reduced. User revocation is also effectively dealt by assigning multi-valued access expiration time.

Keywords

Access Control, Ciphertext policy Encryption, data replication, key structure, User revocation.

Manuscript received February 18, 2014.

Surya Prabha U S, Department of Information Technology, Anna University Chennai, Regional Centre Coimbatore, India.

P Marikkannu, Department of IT, Anna University Chennai, Regional Centre Coimbatore, India.

Arul Vineeth A D, Software Engineer, ECS Financials, Thiruvananthapuram, India.

1. Introduction

Cloud consists of a collection of interconnected and virtualized computer that are actively purveyed and demoed as a unified computing resources based on service level agreements. Cloud provides services to the user irrespective of the infrastructure on which these are hosted. Cloud computing is a model for enabling omnipresent, convenient on-demand network access to a shared pool of configurable computing resources (e.g. server, storage and network) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing is the most dominant epitome in IT industry. Most prominent characteristics are broad network access, resource planning, measured service. Cloud computing achieves economics of scale, streamlines processes, minimize licensing new software, cheap globalization, improve accessibility and flexibility. One of the virtues of the cloud is its potential for real time performance data and on-demand transparency. Security and privacy issues exhibits a strong barrier for users to adapt into cloud computing systems due to its internet based data access and management. As cloud service provider is a commercial enterprise it cannot be trusted and also user depots their data and business operations in service provider. Flexible and fine-grained access control is in demand in service oriented cloud computing irrespective of data confidentiality. Access control is a key concern and ensures that authorized users access a number of cloud data and the system. In cloud system this policy is enforced through access control mechanisms. Before accessing the resources: identification, authorization, authentication, accountability are conducted in access control system. In various access control models, Bell-La Padula (BLP) [3] and BiBa [4] are two famous certified frameworks. Many schemata have been proposed [10]-[12] to achieve flexibility and fine-grained access control. Here a problem arises when data owner and service providers are not in same trusted domain. Since they are not in same trusted domain a new scheme called Attribute Based Encryption ABE [5] proposed by Yu et al [6] which

espouses key-policy attribute based encryption (KP-ABE) to impose fine grained access control.In KP-ABE, attributes are assigned to a ciphertext while creating and policies are assigned to users /key by an authority. Policy here corresponds to a access structure. A key can only decrypt these cipher texts whose attribute satisfy the policy. In Ciphertext-policy attribute based encryption (CP-ABE) [8], a user has various attributes and accordingly receives a key from the trusted authority for its set of attributes. Ciphertext contain a policy. If user's attribute set satisfies the policy, it can use the key to decrypt the ciphertext. Multiple users cannot pool their attributes together.A Hierarchical Attribute Set Based Encryption (HASBE) [1] access control scheme extends the concept of ciphertext attribute-set-based encryption (CP-ABE) with a hierarchical structure of system users, to ensure compromising, scalable, close grained access control. Cloud Service Provider, Trusted Authority, Domain Authority, Data owner, Data consumer are the five entities in the HASBE. A novel business model is proposed based on separate encryption/ decryption and storage. Encryption/Decryption as a Service and Storage as a Service (SaaS) are provided by separate operators.

2. Literature Review

A. Cloud Computing and Emerging IT Platforms

In 2009, RajkumarBuyya, Chee Shin Yeo, SrikumarVenugopal, James Broberg, and IvonaBrandic [2] proposed that,Cloud computing is considered as the 5th utility (after water, electricity, gas and telephony). Architecture of cloud is defined with market oriented resource allocation. Cloud computing expresses business application capabilities as sophisticated services accessed over a network. Through internet, content can be accessed irrespective to host infrastructure. This infrastructure consists of data centres. Data centres are monitored and maintained by content providers. Consumers are charged to access content from the providers which are induced by profit. Consumers are provided with the opportunity to reduce or eliminate cost related service. For core business operations consumers should be guaranteed cloud application from providers. Typically service level agreements furnish this service between providers and consumers.

B. Attribute Based Encryption Methods

In 2006, VipulGoyal, OmkantPandeyy, AmitSahaiz, Brent Waters [5] proposed that, Encrypted files are stored on untrusted server in traditional encrypted file system. Every user can decrypt its own files. A new encrypted file system has label with attributes. The attributes may be file name, file size, date modified of the file, name of the user, Department of the user and so on. In threshold attribute based encryption, Ciphertext has set of attributes, User has set of attributes. If more than k attributes match, user can decrypt the file. The idea of ABE was introduced [9] as a new method for Fuzzy identity-based encryption. ABE schemes are classified into key-policy attribute based encryption (KP-ABE), Ciphertext-policy attribute based encryption (CP-ABE) and Hierarchical attribute set based encryption (HASBE). In a KP-ABE [5], Ciphertext are associated with set of descriptive attributes and private keys are associated with access structures. A user's decryption key is related with a monotonic tree access structure. In a CP-ABE [7], the roles of Ciphertext and decryption keys are switched.
The disadvantages of this method is a problematic security issues arise in nearly every secure system, and particularly in large-scale networked systems such as the Global Information Grid, where diverse secret, top secret and highly classified information will need to appear intermingled in distributed audit logs.

C. HASBE Model

In 2010, R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic [13] proposed that,Cloud an emerging epitome allows users to store their data securely in cloud to enjoy scalable services according to their requirements. Especially small and medium sized endeavour with bounded budgets can save capital with reduced resources but parallely improves performance by using cloud based services to handle their projects. CSPs with control over the data shared, may be completely transparent to endeavour users, which may arouse potential security and privacy issues. To hold the sensible user data against untrusted CSPs, cryptographic approaches are applied by divulging decryption keys only to authorized users. When endeavour users outsource confidential data for sharing on cloud servers, the acquired encryption system should not only support fine-grained access control, but also provide eminent performance, full deputation and scalability.They should assist the needs of accessing data anytime and anywhere, delegating within enterprises and reaching a dynamic set of users. To help enterprises to efficiently share confidential data on cloud servers, a scheme HIBE is introduced. Hierarchical Identity Based Encryption (HIBE) system achieves this goal by combining hierarchical identity based encryption (HIBE) system

and the cipher text policy attribute based encryption (CP-ABE) system.This model consists of a root master (RM) that corresponds to the third trusted party (TTP). Multiple domain masters (DMs) are available, in which the top-level DMs correspond to multiple enterprise users, and numerous users who corresponds to all personnel in an enterprise. The role of RM is to closely follow the root private key generator (PKG) in a HIBE system and is responsible for the generation and distribution of system parameters and domain keys. The role of DM is to integrate both the properties of the domain PKG in a HIBE system and AA in a CP-ABE system and is responsible for deputing keys to DMs at the next level and distributing keys to users. It also enables the leftmost DM at the second level to administer all the users in an arena. Other DMs administer an arbitrary number of disjoint attributes, and controls the whole structure and semantics of their attributes. The HIBE model marks each DM and attribute with a unique identifier (ID), and also mark each user with both an ID and a set of descriptive attributes. Gentry et al enabled an entity's secret key to be extracted from the DM itself and an entity's public key, which denotes its position in the HASBE model. An ID tuple consisting of the public key of the DM administering itself and its ID, e.g., the public key of DMiwith IDiis in the form of (PKi−1; IDi), the public key of user U with IDuis in the form of (PK♢ ; IDu), and the public key of attribute a with IDais in the form of (PKi; IDa), where PKi−1, PK♢ , and PKiare assumed to be the public keys of the DMs that administer DMi, U, and a, respectively. This scheme has several traits: (1) high performance (2) fine-grained access control (3) scalability (4) full delegation. The HASBE scheme, which is also collusion resistant, proves to semantically secure against adaptive chosen plaintext attacks under the BDH assumption and the random oracle model. The disadvantage of this model is that the work is not towards designing a more expressive scheme, so it cannot be proved to have full security under the standard model.The performance is not enough.

3. Access Control Solutions

A. Ciphertext Attribute Set Based Encryption (CPASBE)

In various distributed systems user own a sealed set of credentials or impute to access data. Presently trusted servers impose these policies to store resources and attribute access control. Withal, determine a server that stores data securely then data confidentially is compromised. A system is defined to realize complex access control on encrypted data through Ciphertext Attribute Set Based Encryption (CP-ASBE). The technique makes sure that encrypted data are kept confidential even if the provider is not trustworthy. It secures data against collusion attacks. Former Attribute Based Encryption uses attribute to encrypt a data but in this system user credentials are used to describe the encrypted data and provider decides who to decrypt the data. The method is similar to the traditional access control methods such as Role Based Access Control (RBAC). A user's private key will be associated with a random number of attributes expressed as strings. On other hand, when a user encrypts a message in the system, it specifies a related access structure over attributes. A user will only be able to decrypt a Ciphertext if that user's attributes pass through the cipher text's access structure. At a mathematical level, access structures in the system are described by a monotonic "access tree", where nodes of the access structure are composed of threshold gates and the leaves describe attributes. AND gates can be constructed as n-of-n threshold gates and OR gates as 1-of-n threshold gates.

CP-ASBE supports multiple value assignments for an attribute with a single key. CPASBE [8] scheme organizes user attributes in key thus allowing users to dynamically inflict constraint so as to combine attributes to satisfy policies. The below exemplify key structure of depth 2 is specified for a graduate student in IT department of a university where student is AA for course 01 and has inscribed himself in course 11.Clearly, multiple values can be allotted for the same attribute, here the attribute 'Role' is assigned as "AA" and 'Grad-Student' in various sets.

{Dept: IT, Role: Grad- Student,
{Course ID: 01, Role: AA},
{Course ID: 11, Role: PG-Student}}.

The above example shows that the graduate students holds a private key that should not be able to merge "Role: AA" with course '11' so as to access course grades of students who have enrolled in '11'. This feature can be implemented by combining Hierarchical Identity Based Encryption (HIBE) and CP-ABE. Also the encryptor has to assure that a student cannot select or combine attributes from different sets. ASBE along with CP-ABE solves this problem by assigning multiple values to group of attributes in various sets. Thus ciphertext policy encryption is effectively implemented by ASBE.

B. CP-ASBE Scheme

A common method for protecting sensitive data from third parties is to have data's in data owner itself. A data owner is solely responsible for securing his data. Also replication is avoided. Attribute based encryption turns out to be a good technique for realizing scalable access control solutions. A CP-ASBE system consists of four algorithms: Setup, KeyGen, Encrypt, and Decrypt.

Let Q0 be a bilinear group of prime order p and let q be generator of Q0. Let e: Q0 x Q0→Q1 denotes a bilinear map. Let H: {0, 1}*→Q0 be a hash function that maps any arbitrary string to a random group element.

Setup (d=2): Depth of key structure (d) is input parameter that generates a Public key PK and Master key MK for the scheme.

PK = (Q, q, x1=qβ1, y1=q1/β1, x2=gβ2, y2=g1/β2,e(q,q)α) (1)

MK= (β1,β2.qα) (2)

Here α, βi ϵ ZpVi ϵ {1, 2} are random exponents.

KeyGen (MK, u, S): Secret key SKu for a user U is obtained from the Master key MK, identity of user U and key structure S.

SKu =(S,D=q(α+r{u})/β1,Di,j= qri{u}.H(Si,j)ri,j{u},Di,j = qri,j{u} for 0 ≤ i ≤ m, 1 ≤ j ≤ ni,

Ei =q(r{u}+ri{u}) for 1≤i≤m) (3)

Here Si,j represents jth attribute appearing in set Si. ri{u} ϵ Zp denotes set of m unique random numbers. ri,j{u} ϵ Zp denotes set of unique random numbers for each (i,j).

Encrypt (PK, M, T): Ciphertext CT is generated by Public key PK, a message m and an access tree T.

CT = {T, Ĉ= M.e(q,q)α.v , C =x_1^v, Ĉ = x_2^v, Vi ϵ L , Ci = qgy(0), C'i = H(aH(l)gy(0) , Vkϵ K: Ĉk = x2yx(0)), } (4)

A random variable v ϵZp and gR (0) =S is opted by the algorithm for root node. L denoted set of leaf nodes in T. K denotes set of translating nodes in T.

Decrypt (CT, SKu): Ciphertext and Secret key SKu yields a message m, if the key S associated with the secret key SKu satisfies T, then m is the original. Otherwise, m is null.

Decrypt node (CT, SKu,t,i) = $\frac{e(D_{i,j},Ct)}{e(D_{i,j},C't)}$= e(q,q)ri{u}. gt(0) (5)

4. Attribute Authority Based Access Control

A. System Model

System contains four types of parties Cloud Service Provider, Data Owner, Data Consumer, Attribute Authority and many Subsidiary Attribute Authorities. The model in Figure 1 delineates access control mechanism and hierarchical structure of the user. A method to access data efficiently from cloud without any data replication is cited.

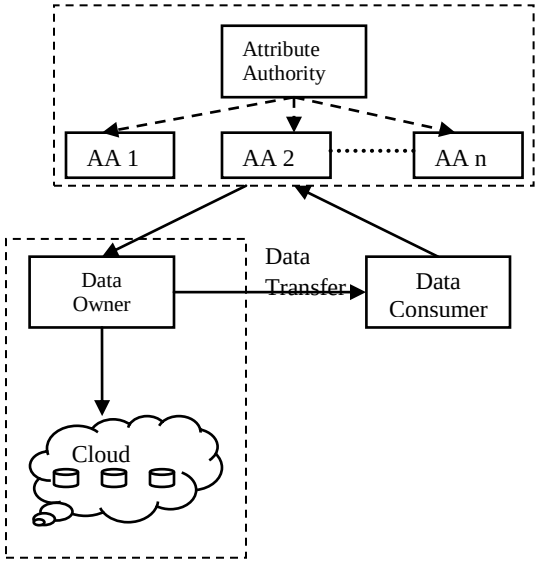

Figure 1: System Model

Cloud Service Provider finagles a cloud to furnish data storage service. Attribute Authority is a root authority and maintains subsidiary attribute authority. AA's role is to verify the level and access control of data consumer. It also manages keys recursively. Data Owners encrypt their data using randomly generated keys by AA. Data Consumer contacts the data owner with the essential contingents needed to access the data. In CP-ASBE, Data owner is always online.

B. Security Model

In Attribute Authority based Data Access initial authentication is provided by a specific Attribute Authority (AA) from a pool of several AA's. As a response, client receives a packet that comprises of a token indicating the authentication from AA's .Data consumer forwards this packet to data owner (acting as server).After receiving the packet an acknowledgement is sent to AA from data owner

requesting for a decryption key. This process helps to detect whether a consumer accessing the data is a rightful user. Once decrypted a single transfer session is established between data consumer and data owner.

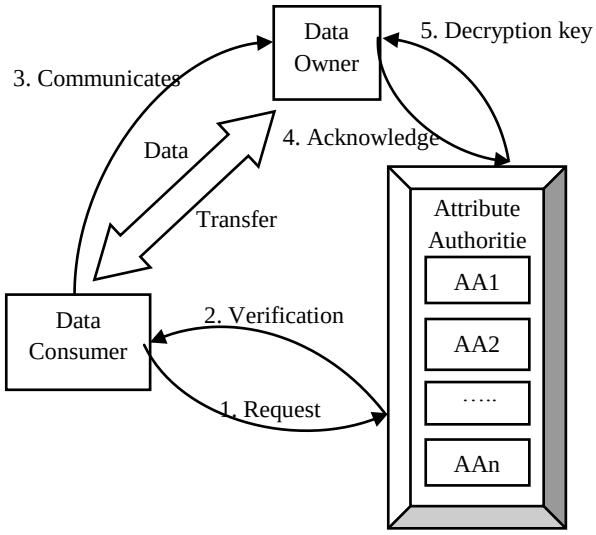

Figure 2: Security Model

5. Performance Evaluation

Comparative study of existing HASBE system and proposed CP-ASBE system was done to measure various aspects of performance improvements of the proposed system. Graphs are plotted to obtain the performance of proposed system over HASBE for access time, security of data shared over cloud and data replication. Figure 3 shows the analysis for access time (in milliseconds) against the number of users accessing the data. The experimental result shows a gradual increase with respect to increasing number of users.

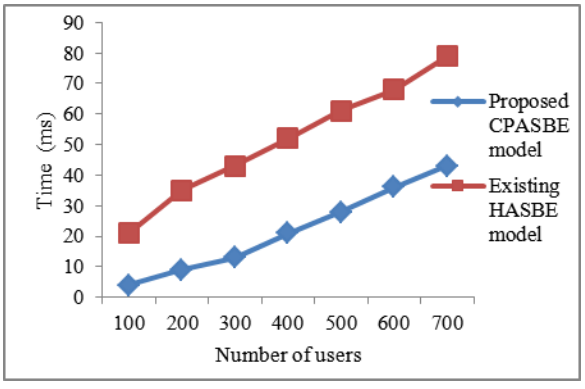

Figure 3: Analysis on access time

Figure 4 compares the surplus data generated against number of files decrypted in kb. In the existing HASBE system the decryption is done by data consumer where the chances of getting access to other data than required are high. But in proposed system the decryption is done by data owner. Here the data consumer can get access only to the required necessary data. This experimental result shows that the proposed system ensures increased security and privacy concerns on the outsourced data.

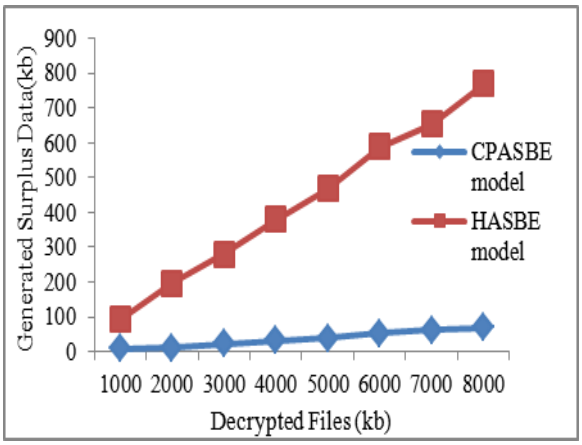

Figure 4: Comparison on generated surplus data

Figure 5 shows the graph for replicated data generated in kb plotted against the size of original source data available. The experimental result shows that the replication of data is very negligible in the proposed system compared to that of the existing technique.

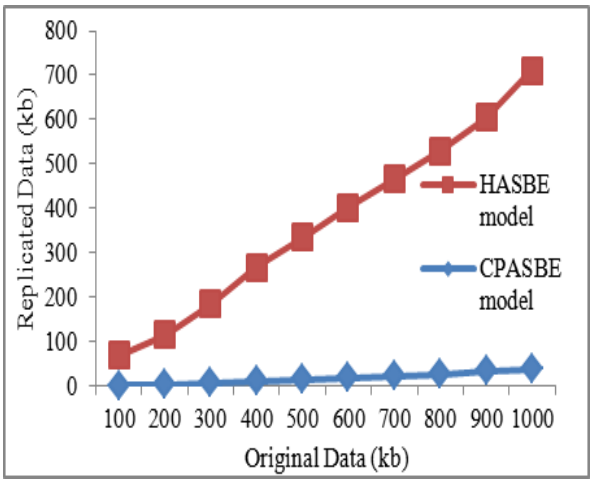

Figure 5: Analysis on generated replicated data

6. Conclusion and Future Work

In this paper, a new hierarchical scheme to realize scalable, versatile and fine-grained access control in cloud is introduced. CP-ASBE achieves effective user revocation because of multiple value assignments. Direct communication between data owner and data consumer reduces overhead in cloud and security of private data's is also enhanced. Thus in this data access scheme replication of original data is fore fended. The proposed system ensures enhanced concealment and security concerns on the outsourced data as the decryption is performed by data owner and furnishes only the requisite data to consumers. In future, various schemes can be used to enhance data distribution time and to optimize usage of resources. Also a novel business model for cloud computing based on a separate encryption and decryption service can be provided to intensify flexibility of the system.

References

[1] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions On Information Forensics And Security, Vol Senior Member, IEEE. 7, No. 2, pp. 743-754, April 2012.

[2] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Comput. Syst., vol. 25, pp. 599–616, 2009.

[3] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech.Rep. 1976.

[4] K.J.Biba, Integrity Considerations for Secure Computer Systems "The MITRE" Corporation, Tech. Rep., 1977.

[5] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria, VA, 2006.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM 2010, pp. 534-542, 2010.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp.Security and Privacy, Oakland, CA, 2007.

[8] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in Proc.ESORICS, Saint Malo, France, 2009.

[9] A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proc.Acvances in Cryptology Eurocrypt, vol. 3494, LNCS, pp. 457-473, 2005.

[10] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. NDSS, San Diego, CA, 2001.

[11] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. IEEE Symp. Security and Privacy, Berkeley, CA, 2002.

[12] T. Yu and M. Winslett, "A unified scheme for resource protection in automated trust negotiation," in Proc. IEEE Symp.Security and Privacy, Berkeley, CA, 2003.

[13] G.Wang, Q. Liu, and J.Wu, "Hierachicalattibute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago,IL, 2010.

Surya Prabha U S received the Bachelor's degree and Master degree in the disciple of Information Technology in 2011 and 2013 from Avinashilingam University For Women and Anna University Chennai, Regional Centre Coimbatore. She is currently doing her research work on security issues and image processing in Cloud Computing.

Dr. P. Marikkannu received his Ph.D (Information and Communication Engineering) from Anna University Chennai and Masters (Master of Technology) in Information Technology from College of Engineering, Guindy, Anna University, Chennai. He is working as an Assistant Professor in the Department of Information Technology, Anna University Regional Centre, Coimbatore. He has published many research articles in various Journals. His research interests include Agent-Based Intelligent Systems, Network Security, Data Mining, Cloud Computing and Distributed Computing. Dr.P.Marikkannu is a life member of ISTE.

A.D. Arul Vineeth received the Master's degree in Information Technology and Bachelor's degree in the disciple of Computer Science and Engineering in 2013 and 2011 from Anna University Regional Centre, Coimbatore and Sun College of Engineering and Technology, Nagercoilaffliated to Anna University, Thirunelveli. He is working as a Software Engineer in the Research and Development Department, ECS Financials, Thiruvananthapuram.