International Journal of Science Engineering and Advance Technology

A Multi-Level Access Control Scheme Towards Software As a Service In Cloud Computing

M. Suneetha[1], G. Vijaya Kumari[2]
[1]M.Tech Scholar, Department of Computer Science & Engineering,
[2]Assosc.Professor, BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.

Abstract—

Cloud computing is a model of data computing, storage, conveyance of services and sharing source assets gave to customers on their request. Rather than obtaining real physical gadgets servers, stockpiling, or any systems administration hardware, client utilized these assets from a cloud supplier as an outsourced benefit. It characterized as a model of administration of data, assets and applications as services over Internet according to prerequisite of clients‖. Cloud processing is a way to deal with helpful and on request arrange access to a shared gathering of registering assets that can be given by specialist organization as different services. It presents another Internet-based condition for on-request access, dynamic arrangement for processing assets by utilizing different compose services on cloud. These models are alluded as Software as a Service, Platform as a Service and Infrastructure as a Service. This paper proposing a system that distinguishes and outline the security and privacy challenges in cloud services. It features cloud-particular assaults and hazards and unmistakably outlines their alleviations and countermeasures. This is likewise feature a multilevel security structure for cloud registering that fulfills security and privacy prerequisites in the clouds and ensure them against gatecrasher assaults. The motivation behind this work is to exhibit and presented a security and privacy viewpoint that will take into contemplations while creating and utilizing the cloud condition either by people or associations.

Keywords: Attribute-Based Access; Access Control. Privacy Preserving, Anonymous authentication.

I. Introduction

Security is one of the clients worries for the adoption of Cloud computing. Moving data to the Cloud generally infers depending on the Cloud Service Provider (CSP) for data insurance. In spite of the fact that this is typically overseen based on lawful or Service Level Agreements (SLA), the CSP could conceivably access the data or even give it to outsiders. In addition, one should confide in the CSP to honestly apply the access control rules characterized by the data proprietor for different clients. The issue turns out to be significantly more mind boggling in Intercloud situations where data may spill out of one CSP to another. Clients may misfortune control on their data. Indeed, even the trust on the unified CSPs is outside the control of the data proprietor. This circumstance prompts reconsider about data security approaches and to move to a data-driven approach where data are self-ensured at whatever point they live. Encryption is the most generally utilized strategy to secure data in the Cloud. Truth be told, the Cloud Security Alliance security direction prescribes data to be ensured very still, in movement and being used. Scrambling data maintains a strategic distance from undesired accesses. In any case, it involves new issues identified with access control administration. A manage based approach would be attractive to give expressiveness. In any case, this assumes a major test for a data-driven approach since data has no calculation capacities independent from anyone else. It can't uphold or figure any access control administer or approach. This raises the issue of strategy choice for a self-secured data bundle: who ought to assess the standards upon an access ask? The main decision is have them assessed by the CSP, however it could possibly sidestep the standards. Another choice is have rules assessed by the data proprietor, yet this infers either data couldn't be shared or the proprietor ought to be online to take a choice for each access ask. To defeat the previously mentioned issues, a few recommendations attempt to give data-driven arrangements based on novel cryptographic systems applying Advanced Cryptographic Standard (ACS). These arrangements are based on Attribute based Access Control (ABAC), in which benefits are conceded to clients as per an arrangement of

attributes. There is a long standing verbal confrontation in the IT people group about whether Role-based Access Control (RBAC) is a superior model for approval. Without going into this level headed discussion, the two methodologies have their own upsides and downsides. To the best of our insight, there is no data-driven approach giving a RBAC model to access control in which data is scrambled and self-secured. The proposition in this framework assumes a first answer for a data-driven RBAC approach, offering a contrasting option to the ABAC demonstrate.

II. Related work

Security and privacy assurance in clouds are being investigated by numerous analysts. Wang et al. [2] tended to capacity security utilizing Reed-Solomon deletion redressing codes. Verification of clients utilizing open key crypto-realistic procedures has been contemplated in [5]. Numerous homo-morphic encryption systems have been recommended [6], [7] to guarantee that the cloud can't read the data while performing calculations on them. Utilizing homomorphic encryption, the cloud gets ciphertext of the data and performs calculations on the ciphertext and returns the encoded estimation of the outcome. The client can decipher the outcome, however the cloud does not comprehend what data it has worked on. In such conditions, the client must be able to check that the cloud returns remedy comes about. Responsibility of clouds is an extremely difficult undertaking and includes specialized issues and law implementation. Neither clouds nor clients ought to deny any tasks performed or asked. It is vital to have log of the exchanges performed; be that as it may, it is an essential worry to choose how much data to keep in the log. Responsibility has been tended to in TrustCloud [8]. Secure provenance has been examined in [9]. Thinking about the accompanying circumstance: A law understudy, Alice, needs to send a progression of reports about a few misbehaviors by specialists of University X to every one of the educators of University X, explore seats of colleges in the nation, and understudies having a place with Law office in all colleges in the territory. She needs to stay mysterious while distributing all confirmation of misbehavior. She stores the data in the cloud. Access control is vital in such case, with the goal that exclusive approved clients can access the data. It is likewise essential to check that the data originates from a solid source. The issues of access control, verification, and privacy assurance ought to be comprehended all the while. We address this issue completely in this paper. Access control in clouds is picking up consideration since it is vital that exclusive approved clients approach legitimate administration. An enormous measure of data is being put away in the cloud, and quite a bit of this is delicate data. Care ought to be taken to guarantee access control of this delicate data which can frequently be identified with wellbeing, vital reports (as in Google Docs or Dropbox) or even individual data (as in interpersonal interaction). There are extensively three sorts of access control: client based access control (UBAC), part based access control (RBAC), and attribute based access control (ABAC). In UBAC, the access control list contains the rundown of clients who are approved to access data. This isn't achievable in clouds where there are numerous clients. In RBAC (presented by Ferraiolo and Kuhn [10]), clients are arranged based on their individual parts. Data can be accessed by clients who have coordinating parts. The parts are characterized by the framework. For instance, just employees and senior secretaries may approach data however not the lesser secretaries. ABAC is more stretched out in scope, in which clients are given attributes, and the data has appended access strategy. Just clients with substantial arrangement of attributes, fulfilling the access approach, can access the data. For example, in the above case certain records may be accessible by employees with over 10 long periods of research involvement or by senior secretaries with over 8 years' understanding. The advantages and disadvantages of RBAC and ABAC are examined in [10].

III. System Model

In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control. The contributions of our scheme are three aspects. Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure. Secondly, we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption. Thirdly, we conduct and

implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FHCP-ABE has low storage cost and computation complexity in terms of encryption and decryption. It should be noticed that the proposed scheme differs from the subsequent CP-ABE schemes, which utilize the user layered model to distribute the work of key creation on multiple domain authorizations and lighten the burden of key authority center. In addition, the part of this work is presented in. The work presented in that conference paper is rough and incomplete, where some important aspects haven‟t been considered. System-In order to achieve secure, scalable and access control on outsourced data in the cloud, we utilize and uniquely combine the following cryptographic techniques. 1. Key Policy Attribute-Based Encryption (KP-ABE). 2. Re-Encryption (PRE) Low Cost: This is the very great advantages for organisations to reduce their cost by having the cloud computing service. Fast Service (Always Up time): Cloud computing service providers having infrastructure so server always in up-time. The amount of decryption code that needs to reside on a resource constrained user device will be smaller. Reduction: Bilinear Decisional Diffie-Hellman, Collusion resistance and can't combine private key components.

Access Controlling Methods: The sensing weather information is transported towards the layer1 which is a type of IaaS cloud service supplied by the cloud provider. The applications can exploit the sensors set up in the cellular devices to capture the elements data the applications need, including temperature value, humidity information, atmospheric pressure and so forth. The information model we present is inspired through the data model suggested, according to which our data model consists by format, device ID, size, time, value and period. How big sensing weather information is based on the raw weather data itself, which signifies how big just one weather data. For time, as lengthy like a mobile phone captures data in the atmosphere where it's in, time the delivering action occurs is going to be considered because the time attribute from the raw sensing data. Something sign represents the most crucial sign of sensing data, this is it means is different from format to format, and different types of cellular devices have different meanings. You can obtain access to the cipher texts only when he/she satisfies the needs.

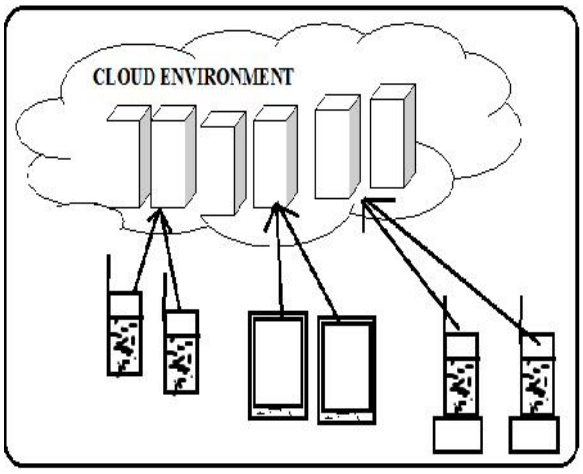

Fig.1.Mobile cloud computing overview

IV. Proposed Methodology

System Framework of FH-CP-ABE: As illustrated in Fig. 1, the system model in cloud computing is given, which consists of four different entities: authority, CSP, data owner and user. In this work, we assume that data owner has k files with k access levels and M ={m1,..., mk }is shared in cloud computing. Here, m1 is the highest hierarchy and mk is the lowest hierarchy. If a user can decrypt m1,the user can also decrypt m2,..., mk . 1.Authority: It is a completely trusted entity and accepts the user enrollment in cloud computing. And it can also execute Setup and KeyGen operations of the proposed scheme. 2.Cloud Service Provider (CSP): It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible. In the proposed system, it provides ciphertext storage and transmission services. Data Owner: It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access structure and executing Encrypt operation. And it uploads ciphertext to CSP. 3.User: It wants to access a large number of data in cloud system. The entity first downloads the corresponding.

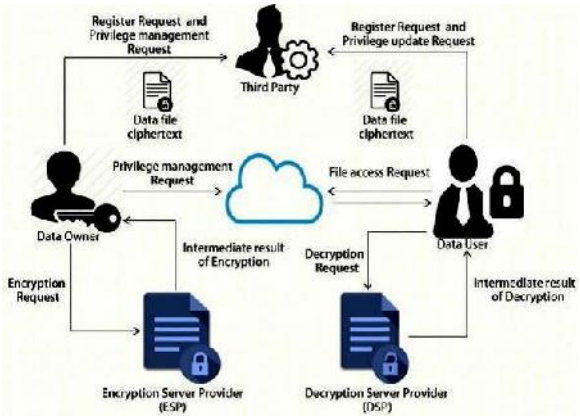

Fig.2 Proposed Architecture diagram

V. Performance Analysis

In this section, the results of theoretical analysis and experimental simulation are given. The experimental results show that the proposed scheme is highly efficient, particularly in terms of encryption and decryption.

To validate theoretical analysis presented in previous subsection, we implement FH-CP-ABE scheme based on the cpabe toolkit and the Java Pairing-Based Cryptography library (JPBC) [42]. The implementation uses a 160-bit elliptic curve group based on the super singular curve y2 = x3+x over a 512-bit finite field. Meanwhile, to compare experimental results of the encryption and decryption, we also simulate the typical CP-ABE [11] system. In addition, the following experiments are conducted by using Java on the system with

Intel Core processor at 2.79 GHz and 1.96GB RAM running Windows XP SP 3. And all of the results are averages of 10 trials.

In the simulation, the FH-CP-ABE scheme's implementation adopts the improved encryption algorithm in encryption operation. As in [40], in a CP-ABE scheme, the complexity of access policy associated with ciphertext impacts two aspects. The one is the time cost of encryption and decryption. The other is the storage cost of ciphertext. To illustrated this, we assume that a patient sets his

PHR's access policy with k access levels in the form of{(a1, a2, . . . , ai , i of i) AND ai+1 . . .AND aN }(i.e., the worst situation over the policy), where each ai (i ∈ [1, N]) denotes an attribute .Meanwhile, the patient generates k policies based the above form for using in CP-ABE scheme. For example, assume that the patient shares three files, i.e., M = {m1,m2,m3}, with three access levels, the access policy is designed as {(a1, a2, . . . , ai ,i of i) AND ai+1 AND ai+2} in FH-CP-ABE scheme. Accordingly, he should construct three access policies for CP-ABE scheme, where the policies are {(a1, a2, . . . , ai , i of i) AND ai+1 AND ai+2}, {(a1, a2, . . . , ai , i of i) AND ai+1}, and {a1, a2, .., ai , i of i }. The policies only contain AND gate to ensure that all the ciphertext components are computed in decryption algorithm. The experimental results are given in Fig. 5. Fig. (a) shows the time cost of encryption and decryption, while Fig. 5(c) shows the storage cost of ciphertext for various attributes with two hierarchy files. Fig. 5(b) and Fig. 5(d) show the time cost and the storage cost for various files with fixed attributes N = 30, respectively. In addition, for various attributes and files, the numbers of attributes and files used in the simulation are N= {10, 15, 20, 25, 30, 35, 40, 45, 50} and k = {2, 4, 6, 8}. As illustrated in Fig. 5(a), we can find that the proposed scheme improves the efficiencies of encryption and decryption greatly when two hierarchy files are shared. We can also find

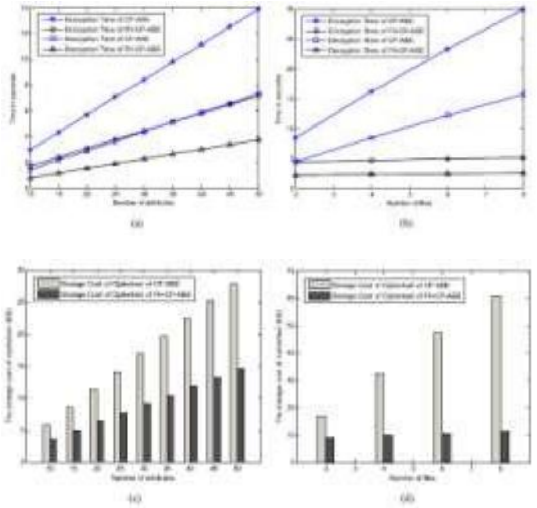

Fig.3. Comparisons between CP-ABE and FH-CP-ABE. (a) Comparison of the encryption and decryption time cost for two files. (b) Comparison of the encryption and decryption cost under 30 attributes. (c) Storage cost comparison of two ciphertext files. (d) Storage cost comparison of multiple ciphertext files under 30 attributes.

that the results are gradually increasing and approximately following a linear relationship with the number of attributes in Fig. 5(a). When the number of files is fixed, the more the number of

attributes is used, the more time cost of encryption and decryption in FH-CP-ABE scheme is saved. For example, in Fig. 5(a), the encryption costs of FH-CP-

ABE and nm CP-ABE scheme are 1.8s and 3s approximately when N = 10.

Similarly, the values are 7s and 14s when N = 50. The difference jumps from 1.2s to 7s when N is changed from 10 to 50. For the storage cost of ciphertext, we find that the value in FH-CP-ABE scheme is smaller than CP-ABE's and follows a linear relationship approximately as the number of attributes grows as shown in Fig. 5(c). If the number of files is fixed, the more the number of attributes is used, the higher efficiency in our scheme is improved in terms of storage cost of ciphertext. For example, in Fig. 5(c), when N = 20 and N = 50, the approximate storage costs of ciphertext are equal to 6.3KB and 14.6KB in FH-CP-ABE scheme, and the values are 11.3KB and 27.8KB in CP-ABE scheme. The saved storage cost is approximately 44.2% and 47.5% with N changed from 20 to 50. When two hierarchy files are shared, the performance of FH-CP-ABE scheme is better than CP-ABE's in terms of encryption and decryption's time cost, and CT's storage cost. The reason is described as below. As shown in Fig. 5(a) and Fig. 5(c), the number of files is k = 2. Based on the Table I, the encryption time in CP-ABE and FH-CP-ABE scheme can be simplified as [2(|AC1|+|AC2|)+2]G0 + 4GT and (2|AC1| + 2)G0 + (2 j |AT| + 4)GT , respectively, where j and |AT | are relatively small in proposed encryption operation. It shows that our scheme can save more encryption time with more common attributes |AC2|. Similarly, the storage cost of CT in both schemes can be denoted as [2(|AC1| + |AC2|) + 2]LG0+ 2LGT and (2|AC1| + 2)LG0 + (j |AT| + 2)LGT , respectively. It indicates that the FH-CP-ABE scheme has smaller storage cost of ciphertext than the CP-ABE in the same condition. In addition, the decryption time for CP-ABE and FH-CP-ABE is approximate to (4|Au| + 2)Ce + [2(|S1| + |S2|) + 4]GT and (2|Au| + 1)Ce + [2|S1| + (j |AT| + 4)]GT , respectively. Obviously ,FH-CP-ABE scheme has lower decryption cost with a same number of common nodes |S2|. So, comparing with CP-ABE and FH-CP-ABE, the encryption cost in our scheme is decreased by (2|AC2|G0 − 2 j |AT |GT) in Fig. 5(a). Similarly, the storage cost of CT and the decryption cost in FH-CP-ABE scheme are reduced by 2|AC2|LG0 − j |AT |LGT) and (2|Au| + 1)Ce + [2|S2| − j |AT |]GT in Fig. 5(c) and Fig. 7(a), respectively, compared to CP-ABE's. The above simulation results also confirm to theoretical analysis described in previous subsection.

As shown in Fig. 5(b), we find that the results of encryption and decryption cost are approximately following a linear relationship as the number of files grows in both schemes. And the values in FH-CP-ABE scheme are smaller than CPABE's at the same condition. This figure shows that the time cost of encryption and decryption to be saved is directly proportional to the number of files to be encrypted and decrypted in FH-CP-ABE scheme when the number of attributes is fixed. For example, in Fig. 5(b), the encryption time of CP-ABE scheme is 8.5s and 30s approximately when k = 2 and k = 8. Accordingly, the parameter in FHCP-ABE scheme is 4.5s and 5.2s. The difference jumps from 4s to 24.8s with k increased from 2 to 8. In addition, we can find that the experiment result of CT's storage cost in FH-CP-ABE is significantly smaller than CP-ABE scheme's for various files with fixed number of attributes in Fig. 7(d). And this figure indicates that the number of files to be encrypted is proportional to the storage cost of ciphertext to be reduced in the proposed scheme. For example, in Fig. 5(d), when k = 4 and k = 8, the approximate storage costs of ciphertext are 9.9KB and 11.4KB in FH-CP-ABE scheme, and the values are 32.6KB and 61KB in CP-ABE scheme. Comparing with CP-ABE and FH-CP-ABE, the reduced storage cost is approximate to 69.6% and 81.3% with k changed from 4 to 8. Above all, when multiple hierarchy files with different access levels are shared, the experiment results indicate that FH-CP-ABE scheme performs better than CP-ABE in terms of the time cost of encryption and decryption, and storage cost of CT, if the number of attributes is fixed. The reason is described as follows. In Fig. 5(b) and Fig. 5(d), the number of attributes is fixed as N = 30. Based on the Table I, the encryption cost in CP-ABE and FH-CP-ABE scheme can be denoted as [2(|AC1| + . . . + |ACk|) + k]G0 + 2kGT and (2|AC1| + k)G0 + (2 j |AT| + 2k)GT, where k = {2, 4, 6, 8} in the simulation, and j and |AT | are relatively small in our proposed scheme. It indicates that FH-CP-ABE requires less encryption time than CP-ABE with more hierarchy files k. Similarly, the CT's storage cost in both schemes can be denoted as [2(|AC1| + . . . + |ACk|) + k]LG0

In Fig. 3(b), the time cost of encryption and decryption in FH-CP-ABE scheme is reduced by [2(|AC2|+. . .+|ACk|)G0− 2 j |AT |GT] and (k −1)(2|Au|+1)Ce +[2(|S2|+. . .+|Sk |)−j |AT |]GT ,

respectively, compared to CP-ABE's. Similarly, comparing with CP-ABE and FH-CP-ABE, the storage cost of CT in our scheme is decreased by [2(|AC2| + . . . +|ACk|)LG0− j |AT |LGT] in Fig. 7(d). Meanwhile, the results are also consistent with theoretical analysis presented in previous Sub section.

VI. Conclusion & Future Work

In this paper, we proposed a variant of CP-ABE to efficiently share the hierarchical files in cloud computing. The hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. Therefore, both ciphertext storage and time cost of encryption are saved. The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files. Moreover, the proposed scheme is proved to be secure under DBDH assumption. This paper contains several encryption schemes for secure sharing of outsourced data in cloud server. From the survey we understand that some amount of work has been done in the field of cloud computing for several security issues. It can be applied to achieve scalable, flexible, security, privacy, data confidentiality and fine-grained access control of outsourced data in cloud computing. The study concludes that the Hierarchical attribute-set based encryption is the advanced encryption scheme for outsourcing data in the cloud service provider. On the other hand the techniques and strategies of encryption in cloud computing have to be improved with its distinct characteristics in mind. There is more scope for future research in the field of secure data sharing in the cloud. In this paper, we analyse different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, HABE and MA-ABE. The main access polices are KP-ABE and CP-ABE, further schemes are obtained based on these policies. Based on their type of access structure the schemes are categorized as either monotonic or non-monotonic. CHABE an adaptation of Attribute Based.

References

[1] Harish shah, Shrikant, Sharma Shankar Anadane, "Security Issues in Cloud Computing".

[2] Ahmad Youssef, "A Framework for secure cloud computing", IJCSI international Journal of Computer Science, Issues, Vol 9, Issues4, N0 3 July 2012, ISSN(Online) 1694-0814, www.IJCSI.org

[3] Ramasami S., Umamaheshwari P., Survey on data security issues and data security model in cloud computing, International Journal of Engineering and Technology (IJEIT), Volume 1, issue 3,March 2012.

[4] Ayesha Malik, Muhammad Moshin Nazir, Security Framework for cloud computing environment : A review, Journal of engineering trends in computing and information sciences, vol. 3 No. 3 March 2012, ISSN 2079-8407.

[5] Wayne A. Jansen, NIST, Cloud hooks: Security and Privacy in cloud computing, Proceeding of the Hawaii International conferences on System Sciences-2011.

[6] Furukawa jun, Furukawa ryo, Mori Kengo, Mori Takuya, Toshiyuki, Araki Toshinor, "A Privacy-Protection Data Processing Solution Based on Cloud Computing", NEC Technical Journal, Vol. 8 No.1, Special Issue on Solving Social Issues through Business Activities

[7] Summathi M, Shravan G.S, Dinesh H.A, Implementation of Multifactor Authentication System for Accessing Cloud Service, International Journal of Scientific and Research Publication, Volume 3, Issues 6, June 2013.

[8] Sh. Ajoudanian , M.R. Ahmadi, "A Novel Data Security Model for Cloud Computing". ISCSIT International Journal of Engineering and Technology, Bol. 4, No. 3, June 2012.

[9] Masayuki Okuhara, Tetsuo Shiozaki, Takuya Suzuki, "Security architecture for Cloud Compting", FUJITSU Sci. Tech. J, Vol 46, No. 4, PP. 397-402 (October 2010).

[10] Ali Newaz Bahar, Md. ahsanHabib, Md. Manowarul Islam, "Security architecture for Mobile Cloud Computing", International Journal of Scientific and Knowledge Computing and Information Technology, 2012-13, IJSK & KAJ, July 2013, Vol. 3 No. 3.

Authors

M. Suneetha is pursing M.TECH (CSE) in the Department of Computer Science and Engineering from BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.

G. Vijaya Kumari is working as Associate Professor in Department of Computer Science & Engineering, BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.