ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Retentive privacy and content based on Location queries

C.Rajeswari[1], N.S.Jagadeesh[2]

M.Tech Student, Dept of Computer Science and Engineering, Kuppam Engineering College, Kuppam, A.P, India [1]

Assistant Professor, Dept of Computer Science and Engineering, Kuppam Engineering College, Kuppam, A.P, India [2]

Abstract: In this paper we present the popularity of location based query services leads to serious concerns on user privacy. The main aim to protect user's database of location data and query privacy issues. The master of the location information that's, the location server, will not desire to purely send out it's information to all or any people. The location server really wants to possess some handle over its information, considering that the information is actually its asset. We suggest a foremost enhancement providing AES Algorithm security on user security and server security for previous solutions by introducing**,** the 2 phase method, where the initial step is dependent on oblivious Transfer and the next step is dependent on private information Retrieval, to obtain any risk-free solution intended for the two parties. The solution many of us existing is actually successful and functional in most situations. We implement this solution on mobile devices and desktops. We also implement the Security Model and analyse the security in the context of our protocol, finally we provide the privacy.

Keywords: Location based query, location server, private information retrieval, oblivious transfer.

I. INTRODUCTION

Location-based services (LBS) are a basic type connected with computer program-level services in which utilize spot data to manipulate characteristics. As such LBS is surely an information service and has quite a few uses in social media today being an entertainment services, and that is accessible having mobile devices through the portable network as well as which in turn utilizes home elevators this geographical placement in the portable system. It's come to be an increasing number of important with the development in the smart phone as well as supplement markets likewise. LBS are used in several contexts, for instance health and fitness, indoor thing look for, entertainment, do the job, private living, and many others. LBS incorporate services to name a location of your individual or maybe thing, for instance getting this nearest ATM or maybe this whereabouts of your good friend or maybe worker. LBS incorporate package checking as well as car checking services. LBS normally include portable trade as soon as using the design connected with discount coupons or maybe promoting directed at consumers dependant on the existing spot. They will incorporate personal weather services and in some cases location-based game titles.

Spot Primarily based Solutions are a component of virtually all command and also plan devices which often do the job within computer systems currently they have got evolved by easy synchronization structured program designs in order to authenticated and also sophisticated methods pertaining to employing almost any spot structured program product or even facility.

LBS will be to be able to start and also near distinct information things based on the utilization of area and/or period because (controls and also triggers) or even in complex cryptographic important or even hashing programs as well as the information they provide use of. Location based providers these days are usually part of sets from management programs to be able to intelligent weaponry. They are definitely applied trillions of times a day and may become probably the most greatly applied application-layer conclusion composition inside processing these days.

In any case, there are sure issues while utilizing LBS that it may gather and utilization unlimited measure of data about buyer for an extensive variety of reason. Area data is delicate and clients would prefer not to share such data to conniving LBS servers. Since number of noxious foes may get more private learning of the clients. Likewise, questions fire by the client having touchy data about people, including wellbeing condition, way of life propensities. So he wouldn't like to uncover it. Protection concerns are relied upon to ascend as LBSs turn out to be more normal. Area protection implies information security. So here security certification is measure issue. On the other, area server has their own particular database in which, number of purpose of interest records are found (fig.1) the server transform the solicitation and sends back the inquiry result to the client. So server needs to keep database access from unapproved client furthermore clients who have not pay for that administration.

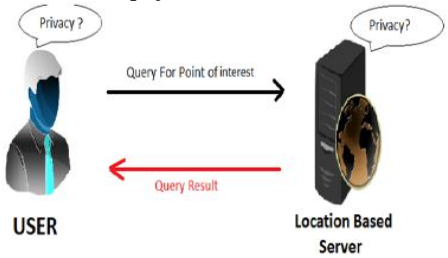

Fig.1 Location based service process

DOI 10.17148/IJARCCE.2015.4973

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Number of existing framework utilized conventions for security of Location based administrations. Be that as it may, we need to secure three things i) area protection ii) query protection iii) database protection.
The rest of the paper is arranged as follows. In part II we surveys the related work that pointing area based administrations and conventions identified with LBS part III will be our proposed work and part IV concludes our function and gives future improvement bearings.

II. RELATED WORK

The primary answer for the issue was proposed by Beresford [1], in which the client's protection is kept up by continually changing the client's name or nom de plume inside of some mix zone. It can be demonstrated that, because of the information's way being traded between the client and the server, the successive changing of the client's name gives little assurance to the client's security. A later examination of the mix zone methodology has been connected to street systems. They explored the obliged number of clients to fulfil the unlink capacity property when there are rehashed questions over an interim. This obliges cautious control of what number of clients is contained inside of the mix zone, which is hard to accomplish by and by.
There are various methodologies in the writing to take care of the issues of security insurance with area based administrations which incorporates shrouding, era of shams and private information retrieval (PIR). A correlative system to the mix zone methodology is in light of k-anonymity [2]. The idea of k-anonymity was presented as a system for protecting security when discharging delicate records [3]. This is accomplished by speculation and concealment algorithms to guarantee that a record couldn't be recognized from (K – 1) different record.
With this innovation it includes one idea anonymiser which is trusted outsider. A client sends its area, inquiry and K to the anonymiser, which is a trusted outsider in unified frameworks or a companion in decentralized frameworks. The anonymiser evacuates the client's ID. TTP recover shroud for client area by making K-anonymise spatial district in which number of k-1 clients are included. At that point anonymiser sends the K-ASR and question to the LBS disjoin, which ascertains the competitor results appreciation to the shrouded locale and sends them back to the anonymiser. At that point the anonymiser which knows the areas of the considerable number of clients computes the real results and sends them back to the client
There is an improvement of this framework that is somewhat sending all Cloaked Region (CR) to server, an anonymiser just sends a focal point of K-anonymizing spatial locale (K-ASR). Yet there are disadvantages in K-obscurity (i) if aggressor specifically picks up the entrance of anonymiser; the protection of all clients is traded off. (ii) At slightest least client ought to subscribe, generally CR can't be developed. (iii) User redesigning is another for making timing districts. (iv)If client flame inquiry out of the timed locale, he can be effectively recognized in light of the fact that he will be incorporated in all CRs. With the utilization of a focal anonymiser are not functional, Hashem and Kulik displayed a plan whereby a gathering of trusted clients build a specially appointed system and the errand of questioning the LS is designated to a solitary client.

Another system for evading the utilization of a trusted anonymiser is to utilize "sham" areas [4]. These techniques propose to produce sham directions with a specific end goal to confound the foes. In that when client can inquiry to server with their portable area and parameters, it can be changed over into another question having client's genuine area and k-1 fake areas and their parameters. Be that as it may, watch that, security is not ensured by supplanting the genuine client personality with fake one in light of the fact that so as to process area ward inquiries, the LBS needs the accurate area of questioning client.

The vast majority of the issues are determined by presenting (PIR) Private Information Retrieval [5]. The essential thought is to utilize PIR to empower the client to question the area database without trading off the protection of client .Existing framework requires timed locale and a TTP, however it doesn't need of anonymiser and security is accomplish through cryptographic methods. Here server shapes the locale with respect to POI keeping in mind offering an explanation to question, server first send districts to client. The client finds the district that contains him and uses PIR to demand all focuses inside of that locale. Thus, the server does not know which area was recovered. This system is excessively lavish, making it impossible to actualize and CPU usage is likewise high and more over client need to invest energy for inquiry execution.
This proposal was stretched out to give database security. This convention comprises of two stages. In the first stage, the client and server use homomorphic encryption to permit the client to secretly figure out if area is contained inside of a cell, without uncovering directions to the server. In the second stage, PIR is utilized to recover the information contained inside of the proper cell. The homomorphic encryption plan used to secretly think about two whole numbers is the Paillier encryption plan. The Paillier encryption plan [6] is known not additively homomorphic and multiplicatively-by-a-steady homomorphic. This implies that we can include or scale numbers notwithstanding when all numbers are scrambled. Both elements are utilized to focus the sign (most critical bit) of (a − b), and thus the client has the capacity focus the cell in which he/she is situated, without uncovering area.

III. PROPOSED WORK

In this paper, we propose a novel convention for area based inquiries that have significant execution changes concerning the methodology by Ghinita at el. [7] and [8].Like such convention; our convention is sorted out as per two stages. In the first stage, the client secretly decides his/her area inside of an open lattice, utilizing

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

careless exchange. This information contains both the ID and related symmetric key for the piece of information in the private network. In the second stage, the client executes a communicational proficient PIR [9], to recover the fitting piece in the private matrix. This square is unscrambled utilizing the symmetric key acquired as a part of the past stage. Our convention therefore gives security to both the client and the server. The client is ensured on the grounds that the server is not able to focus his/her area. Thus, the server's information is ensured since a pernicious client can just decode the piece of information got by PIR with the encryption key gained in the past stage. At the end of the day, clients can't increase any more information than what they have paid for. We comment that this paper is an upgrade of a past work [10]. Specifically, the accompanying help is made.

1. Redesigned the key structure
2. Added a formal security model
3. Implemented the arrangement on both a cell phone and desktop machine

Likewise with our past work, the finishing exhibits the effectiveness and authenticity of our methodology.

3.1 System Model

The framework model comprises of three sorts of elements (see Fig. 2): the arrangement of clients who wish to get to area information, a portable mobile service provider SP, and an location server LS. From the perspective of a client, the SP and LS will form a server, which will serve both capacities. The client does not should be worried with the correspondence's specifics. The clients in our model utilize some area based administration gave by the location server LS. For instance, what is the closest ATM or location? The reason for the versatile service provider SP is to set up and keep up the correspondence between the area server and the client. The location server LS possesses an arrangement of POI records, this portrays a POI, giving GPS directions to its area.

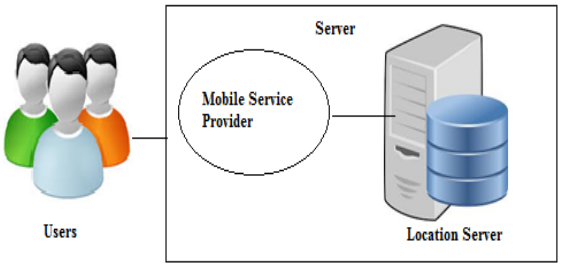

Fig.2 System Model

3.2 Protocol Model

The conclusive objective of our convention is to get a set (piece) of POI records from the LS, which are near the client's position, without trading off the client's security or the information put away at the server. We accomplish this by applying a two stage methodology demonstrated in Fig. 3. The primary stage is in light of a two-dimensional neglectful exchange [12] and the second stage is in view of a communicational effective PIR [13]. The negligent exchange based convention is utilized by the client to get the cell ID, where the client is found, and the relating symmetric key. The cell's learning ID and the symmetric key is then utilized as a part of the PIR based convention to acquire and unscramble the area information. The client decides his/her area inside of a freely produced framework P by utilizing his/her GPS facilitates and shapes a careless exchange query2. The base measurements of general society lattice are characterized by the server and are made accessible to all clients of the framework. This open framework superimposes over the secretly apportioned network produced by the area server's POI records, such that for every cell Qi,j in the server's allotment there is no less than one Pi,j cell from general society matrix. Since PIR does not oblige that a client is compelled to acquire stand out bit/hinder, the area server needs to execute some insurance for its records. This is accomplished by encoding every record in the POI database with a key utilizing a symmetric key algorithm, where the key for encryption is the same key utilized for decoding. This key is expanded with the cell information recovered by the neglectful exchange inquiry. Thus, regardless of the possibility that the client utilizes PIR to get more than one record, the information will be good for nothing bringing about enhanced security for the server's database. Before we depict the convention in point of interest, we portray some introduction performed by both sides.

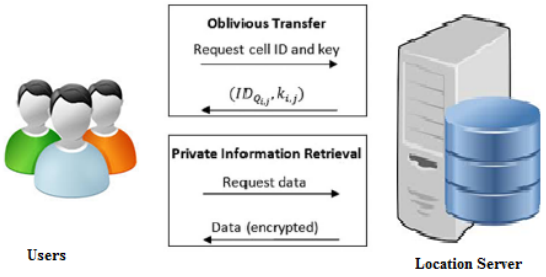

Fig.3 High Level Overview of the Protocol

3.2.1 Oblivious Transfer Based Protocol

The reason for this convention is for the client to get one and stand out record from the cell in people in general framework P. We accomplish this by developing a 2-dimensional neglectful exchange, in view of the ElGamal Oblivious exchange [14], utilizing versatile careless exchange proposed by Naor et al [15]. General society network P, known by both sides, has m segments and n columns. Every cell in P contains a symmetric key ki,j and a cell id in network Q or (IDQi,j , ki,j), which can be spoken to by a surge of bits Xi,j. The client decides i, j organizes in the general population lattice which is utilized to procure the information from the cell inside of the matrix. The convention is introduced by the server.

3.2.2 Private Information Retrieval Protocol

The data about which cells are contained in the private matrix are known, and the key's learning that scrambles the information in the cell, the client can start a private data recovery convention with the area server to

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

get the encoded POI information. Accepting the server has introduced the whole number e, the client ui and LS can take part in the accompanying private data recovery convention utilizing the IDQi,j , got from the execution of the past convention, as information. The IDQi, j permits the client to pick the related prime number force πi, which thus permits the client to question the server.

3.3 Security Analysis

3.3.1 User's Security

The client would not like to reveal the cell Pi, j which contains area to the server. Two presumptions must be kept up keeping in mind the end goal to successfully render area private. The server should not have the capacity to figure out which cell the client is questioning in unaware exchange convention, and the server should not have the capacity to figure out which cell the client is questioning in private data recovery convention. The unaware exchange suspicion is in light of discrete algorithm presumption. This basically implies the given gx (mod p), where p is substantial prime and g is generator of some cyclic gathering, it is computationally infeasible to focus x. For our situation, if the client supplies (g1r1, g1-iy1r1) and (g2r2, g2-iy2r2) to the server, then the server is not able to focus i and j. On the off chance that the discrete algorithm presumption holds, then we guarantee this is secure.

3.3.2 Server's security

The server' security is in light of keeping the limits of its records private. Since uncovering this data may empower the client to deduce more data about the database than he/she is permitted. In our answer this data is secured by negligent exchange convention. The client is compelled to recover one and one and only record from the open lattice Pi,j every other time, the outcome will be indistinct from irregular. Under the discrete algorithm issue presumption, it is computationally obstinate to focus any example from figure content; subsequently, the client is just ready to focus one and one and only result.

3.4 AES Algorithm

The source node might want to send information for the destination around then we perform the security achievement, before sending the information to the destination the source node can impart the security key to the assistance of AES algorithm, subsequent to sharing the key the source node can scramble the information by utilizing cryptographic algorithm. Encoded information exchanged from source to destination, amidst transmission the assailants through middle of the road nodes need to get to the information there will be no impact on the information, because of scrambling the information, the first information as it is send to its destination node. The destination node decodes the information from cipher content to plain content. For giving the security we utilize the exceptionally created Encrypted Standards Algorithm. AES algorithm is a symmetric key algorithm, which implies that comparative key is utilized for encryption and decoding of information.

All of us suggest AES algorithm would be the advanced encryption standard type of algorithm that's recently been utilized to be a symmetric type of encryption. This kind of algorithm will be utilized by different programs. This AES algorithm is seen with in 3 various kinds of black ciphers are present as well as one of these will be utilized to execute different things to do. This several varieties of AES algorithm usually are AES-128, AES-192 in addition to AES-256. Every one of the black cipher may be employed for the explanation of needing some form of colour touch and that is mostly used to be a prohibit dimensions while using collection connected with numerous important factors and also other equipment with them. This AES algorithms experienced grow to be thus well known that they're used simply by some people at any time and as such it's widely used.

They were observed to be genuinely useful to the general population and it additionally joined with the information encryption strategy as well. It has been discovered that the 128 bits piece size is the settled size of square that is being utilized by numerous individuals. Besides substitution variety system is the main coordination which is being utilized as a part of the AES algorithm and it likewise been utilized with the end goal of adding to an outlines' percentage and also. AES algorithm is additionally upheld to be utilized by the state which had been inherent the type of a 4*4 size. Then again the figure content which is contained in the AES algorithm can likewise be utilized as a mean of providing so as to create some level of yield some amount of info to it. A few sorts of steps had additionally been created for the standard of touching base at the AES algorithm and every stride is in charge of performing an undertakings' percentage.

3.4.1 Key Expansion

Round keys are derivative from the cipher key using Rijndael's key schedule.To create round keys for each round, AES algorithm uses a key expansion process. If the number of rounds is N_r, the key-expansion routine creates N_r + 1 128-bit round keys from one single 128-bit cipher key.

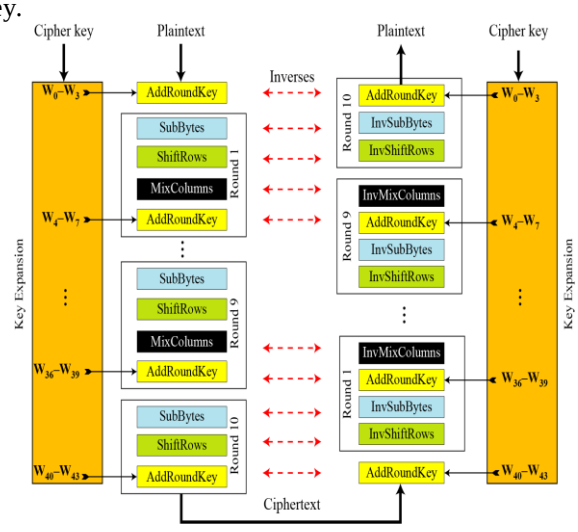

Fig.4 Architecture of AES

3.4.1.1 Initial Round

Add Round key for every byte of the state is combined with the round key using bitwise XOR.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

3.4.1.2 Rounds

1. Sub bytes are non-linear replacement step where each byte is replaced with another according to a lookup table.
2. Shift Rows-a transposition step where each row of the state is shifted cyclically a certain number of steps.
3. Mix columns- a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. Add Round Key transformation adds the round key with the block of data.

3.4.1.3 Final Round (no Mix Columns)

Sub Bytes
Shift Rows
Add Round Key

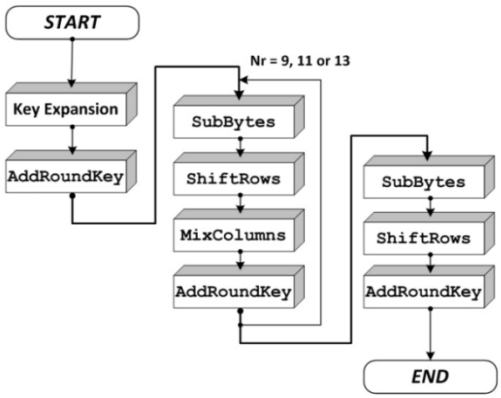

Fig. 5 Key Expansion of Rounds

3.4.2 Algorithm

Cipher (In block [16], one block [16], and word [0….43])
{
Block to state (In block, S)
S← Add Round key(S, W [0…..3])
For (Round=0to 9)
{
S← sub bytes(S)
S← shift rows(S)
If (Round≠9), S← mix column(s)
S← Add round key(S, W [4*round, 4*round+3])
}
State to block (S. out block);
}

Round	*Words*			
Pre-round	w_0	w_1	w_2	w_3
1	w_4	w_5	w_6	w_7
2	w_8	w_9	w_{10}	w_{11}
. . .	. . .			
N_r	w_{4N_r}	w_{4N_r+1}	w_{4N_r+2}	w_{4N_r+3}

Table.1 Round Table

IV. CONCLUSION

We have exhibited an area based query arrangement that utilizes two conventions that empowers a client to secretly build up and secure area information. The starting step is for a client to secretly choose his/her area utilizing unaware exchange on an open matrix. The second step includes a private information retrieval association that recovers the record with high correspondence productivity.

We investigations the presentation of our convention and observed it to be both computationally and communicational more which the latest arrangement is. We executed a product model utilizing a desktop machine. The program prototype demonstrates that our project is at useful restrictions.

ACKNOWLEDGMENT

I got success in completing this work by the extreme guidance of my guide, friends and parents. I thanks to them.

REFERENCES

[1] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan.–Mar. 2003
[2] C. Bettini, X. Wang, and S. Jajodia, "Protecting privacy against location-based personal identification," in *Proc. 2nd VDLB Int. Conf. SDM*, W. Jonker and M. Petkovic, Eds., Trondheim, Norway,2005, pp. 185–199, LNCS 3674.
[3] L. Sweeney, "k-Anonymity: A model for protecting privacy," *Int. J. Uncertain. Fuzziness Inowl. Based Syst.*, vol. 10, no. 5,pp. 557–570, Oct. 2002
[4] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proc. 3rd Int. Conf. Pervasive Comput.*, H. Gellersen, R. Want, and A. Schmidt, Eds., 2005, pp. 243–251, LNCS 3468
[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan,"Private queries in location based services: Anonymizers are not necessary," in *Proc. ACM SIGMOD*, Vancouver, BC, Canada, 2008, pp. 121–132.
[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. EUROCRYPT*, vol. 1592, Prague, Czech Republic, 1999, pp. 223–238.
[7] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "A hybrid technique for private location-based queries with database protection," in *Proc. Adv. Spatial Temporal Databases*, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, 2009, pp. 98–116, LNCS 5644.
[8] G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino, "Approximate and exact hybrid algorithms for private nearestneighbor queries with database protection," *GeoInformatica*, vol. 15, no. 14, pp. 1–28, 2010.
[9] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in *Proc. ICALP*, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.
[10] R. Paulet, M. Golam Kaosar, X. Yi, and E. Bertino, "Privacypreserving and content-protecting location based queries," in *Proc. ICDE*, Washington, DC, USA, 2012, pp. 44–53.
[11] G. Ghinita, C. R. Vicente, N. Shang, and E. Bertino, "Privacypreserving matching of spatial datasets with protection against background knowledge," in *Proc. 18th SIGSPATIAL Int. Conf. GIS*, 2010, pp. 3–12.
[12] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in *Proc. CRYPTO*, vol. 1666, Santa Barbara, CA, USA, 1999, pp. 791–791.
[13] C. Gentry and Z. Ramzan, "Single-database private information retrieval with constant communication rate," in *Proc. ICALP*, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., Lisbon, Portugal, 2005, pp. 803–815, LNCS 3580.
[14] M. Bellare and S. Micali, "Non-interactive oblivious transfer and applications," in *Proc. CRYPTO*, 1990, pp. 547–557.
[15] M. Naor and B. Pinkas, "Oblivious transfer with adaptive queries," in *Proc. CRYPTO*, vol. 1666, Santa Barbara, CA, USA 1999, pp. 791–791.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

BIOGRAPHIES

C.RAJESWARI, pursuing M.Tech in CSE with Specialization Computer Science and Engineering from Kuppam Engineering College, Kuppam Affiliated to JNTUA.

N.S.JAGADEESH, currently he is working as Assistant Professor in Kuppam Engineering College, kuppam, received B.Tech (Information Technology) and M.Tech (Computer Science and Engineering) from JNTU-A, Anantapur. His Research interest areas are Data warehousing and Mining & Cloud Computing, Software Engineering.