

# ENHANCING SECURITY IN E-HEALTH CLOUDS BY AUGMENTING TIMESTAMP AND CONJUNCTIVE KEYWORD SEARCH

DURGAVAJJALA PRATHIMA<sup>#1</sup>, DR. KUNJAM NAGESWARA RAO<sup>#2</sup>

<sup>#1</sup> M.Tech Scholar, Department of Computer Science and System Engineering,  
Andhra University College of Engineering (A), Visakhapatnam, AP, India.

<sup>#2</sup> Associate Professor, Department of Computer Science and System Engineering,  
Andhra University College of Engineering (A), Visakhapatnam, AP, India.

## ABSTRACT

Now a day's electronic health (e-health) record (EHR) system becomes an important application that will bring great convenience especially in the healthcare domain. This mainly came into existence in order to give security for the sensitive information of the patients who want to retrieve the information from the concern hospitals. In general the search which is done in e-health records always retrieved in plain text manner, which has no security for the user records. So in order to provide security for the search function, a searchable encryption (SE) scheme was designed in order to incorporate security protection and favorable operability functions together, which can play an important role in the e-health record system. So, a cryptographic primitive named as novel conjunctive keyword search was introduced with designated tester and timing enabled proxy re-encryption function (NRe-dtPECK), which is a kind of a time-dependent SE scheme. It could enable the patients to operate their records for a certain limited time period to search the record. In this application we can restrict the time period based on each and every individual file and the user based. Moreover, the user could be automatically depreciated their access and access priority after a specified period of effective time. The main motto of this paper is to give high level of security for the medical or health records by encrypting the data before it is stored inside the server and also security can be provided by limiting the access for certain period of time so that, the user can't able to use the same access for a long period of time. By conducting various experiments on the proposed model we finally came to an conclusion that this is the first time to implement such a Re-dtPECK method into the cloud for providing security for the sensitive data which is to be stored into the cloud in a secure manner.

## KEY WORDS

Electronic Health Record, Data Security, Re-Encryption Function, Timing Enabled Proxy Server, Searchable Encryption.

## 1. INTRODUCTION

In recent days cloud computing has entered in each and every domain for storing the valuable data of either an individual or organization data. Recently the cloud entered into the medical related information storage unit and named as Care Cloud/Health Care Cloud. Where this is mainly monitored and established under a privately held corporation with collaboration of cloud service provider for data management, EHR record management, billing software's for medical, hospitals and a lot more services[1]. This care cloud is operating all its information from Boston, Massachusetts and its main headquarters is situated in Miami, Florida[2]. This private service mainly offers the medical related people with a service like Software-as-a-Service (SaaS) and also with a novel service like RCM for revenue management of a company. As per the recent survey more that 60 medical representative organizations across 40 states [3] are using this cloud service for medical information storage and they all achieved data access in a efficient manner.



**FIGURE 1. REPRESENTS THE FUTURE CLOUDS ESPECIALLY IN E-HEALTH INFORMATION STORAGE**

From the above figure 1, it can be clearly identify that almost the future clouds is mainly depending on E- services like e-book learning-cloud office and e-health care and so on. The data which is stored in one server can be accessed remotely from other devices in a secure manner. As we all know that now a day's all the users are concentrating more and more in storing their valuable data into the cloud server either public or private clouds, even though there are some limitations that are present in current cloud server. One among the most critical problem what the cloud users are facing is all the data which is

inserted into the cloud is stored in the normal way or in the form of plain text without any encrypted manner. So as the data which is uploaded in the cloud is not stored in our own PC rather than it will be stored in a remote PC, there is no level of achieving data integrity in the current cloud service providers. So in order to resolve this current limitation in the present cloud service providers a new facility like encryption of data is implemented before it is stored into the cloud server, and for this project DRIVEHQ service provider is used as a backend storage cloud for storing the encrypted data into the cloud with this application. Along with this another major limitation which is present in the cloud server is: once the file which is uploaded into the cloud server, it is not having any restrictions like file should open or accessed for only limited users or it should be accessed only for limited time period [4].

As the above restrictions are not available in the current cloud service providers, there is a chance that un-authorized users can able to access the files from cloud server by performing some insider guessing attacks. So the main idea to start this is to provide high level of security for the medical/sensitive data by providing access restrictions for the cloud users for accessing the files within certain period of time not all the time and this will in-turn leads to block the un-authorized file access by the intruders who try to create a insider attack on our sensitive data [5].

## **II. RELATED WORK**

In this section the assumption and system models that was used in our proposed application are discussed in order to propose the Enhancing Security in E-Health Clouds by Augmenting Timestamp and Conjunctive Keyword Search. Now going into the details:

### **MOTIVATION**

In this section the E-Health Records and also about the advantages of health care cloud are discussed.

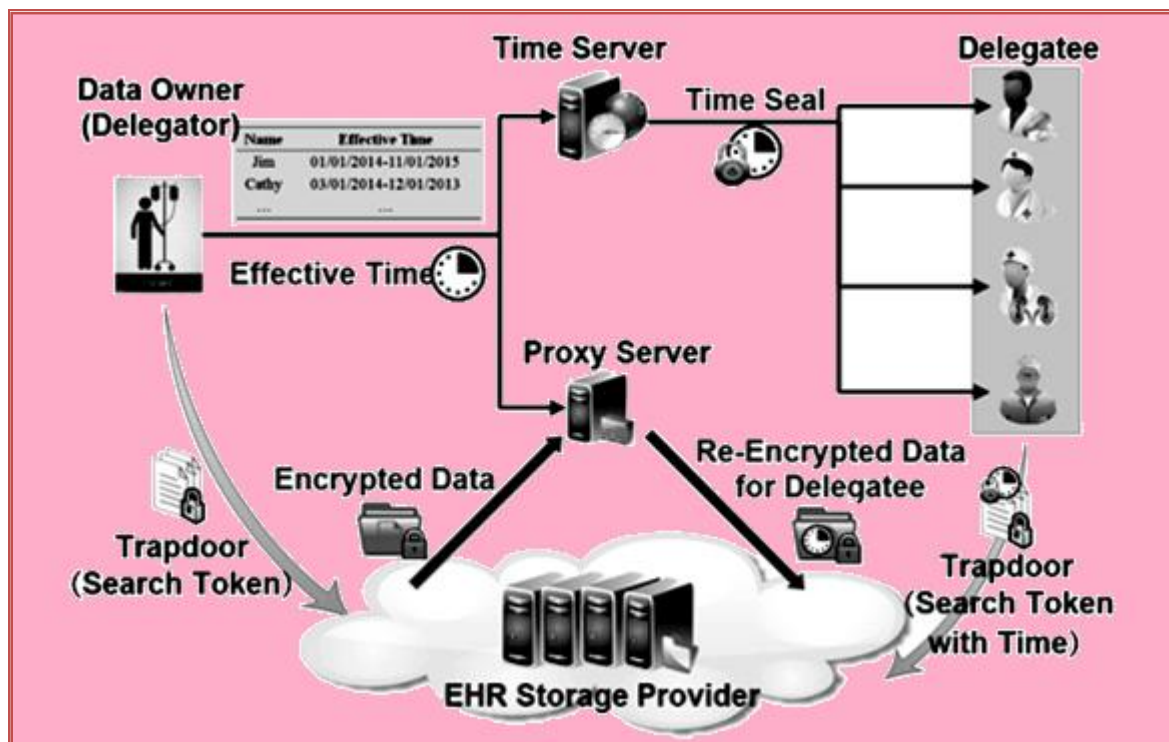
The Electronic Health Records (EHR) system is designed in order to store all the medical records in a computerized manner with the help of some medical software's in order to prevent or avoid the medical errors [6]. The main advantage of using this EHR is it will allow a patient to build his/her own health information in one hospital and has the ability to share the same information with other hospitals. Till now there were a lot of practical patient-centric EHR systems have been implemented so far like Google Health, Care Cloud Server and Handy Patients Enterprise Edition tool and so on [7]. Patient's records can be inserted into the cloud server. The data which is stored in the healthcare information exchange servers mainly contain private or sensitive information, it must not be disclosure to the health care individuals or health care companies who try to gather such information for their personal need and in turn gain profits by leaking that information to others[8]. Even though the cloud care or EHR service providers try to convince the patients to believe that the privacy information will be safekeeping, the EHR could be exposed if the server is intruded or an inside staff misbehaves. The serious privacy and security concerns are the overriding obstacle that stands in the way of wide adoption of the systems.

From the medical records in cloud, a view of an EHR for a patient can be identified, where in that full information can be examined and the positions of various parts can be identified and try to maintain all the information about that patient in the ehr[9]. With this a clear idea can be formed that electronic health reports are mainly used to store each and every sensitive information about the patient inside the cloud server and this information need to be stored in a secure manner. EHR systems are mainly designed

to store data effectively and in a accurate manner to record or identify the status about the patient over time. It is used mainly for verifying all the case history details about the patient previous medical records that are available with him and this will reduce a lot of paper work manually[10].

### III. THE PROPOSED NRE-dtPECK ALGORITHM

In this section, the proposed NRE-dtPECK algorithm for storing the individual private EHR files on a third-party database in a secure manner is mainly discussed. Now let us discuss about this architecture in detail as follows:



**FIGURE 2. REPRESENTS THE PROPOSED ARCHITECTURE OF AN EHR STORAGE PROVIDER FOR SECURE DATA STORAGE INTO THE CLOUD**

From the above figure 2, we can clearly represent the proposed architecture flow diagram of current thesis which will mainly discuss about the Timing Enabled Proxy Re-encryption Searchable Encryption Model. Where it contains totally five important roles like

1. Data Owner (Delegator)
2. Semi Trusted Cloud Server (EHR Storage Provider)
3. Data Users(Delegatee)
4. Proxy Server
5. Time Server

In the proposed application the data owner or delegator tries to upload his valuable and sensitive information about his own EHR files on a third-party database (i.e. especially in the cloud server or EHR server database). Now the data owner initially sends the files to the EHR server database with initial level of encryption for that private data, now the EHR server will try to extracts the main keywords that are kept for those EHR files and encrypts those plaintext keywords into the secure searchable indices. Now

the EHR files are also encrypted and in turn converted into ciphertext. Then, that information is stored into the EHR storage provider's database in a secure manner.

Now once the data center or ehr storage provider receives the data from the data owner, it will then allow the user to access the file information for a nominal time period like one day by default .Here whenever any data owner try to upload the files into the data center, the data can be viewed by the data users or delegatee for a limited period of time not all the times. Here by default the accessing time is kept for twenty four hours from the day of upload. Once the date and time of server is crossed the specified time period, the file cannot be accessed by the delegatee even if the file is available in the cloud server. Hence the data users who want to access the file with their valid credentials need to substitute their valid credentials within the time period and they in turn try to access the information in a plain text manner. If the same user or new user who want the same file from cloud server to be accessed for some excess time period after the file permissions are expired, then they need to request the data owner for providing extended time period for file access[11].

Each and every data user /delegatee try to generate a trapdoor to search the EHR files which are provided access to him by using his/her own private key and sends it to the search servers. After receiving the request, the search servers interact with the EHR storage provider to find the matched files and returns those retrieved information to the user in an encrypted form. Here the EHR storage provider will try to check the user request is having timer enabled or disabled for the corresponding file which is requested by that data user. If the corresponding file is having access permission enabled, then the file can be downloaded directly in a plain text manner by that concern delegatee. If the same file is already expired from the storage server , then the data owner try to send a request to the proxy server for enabling him the re-encryption facility. Here the term re-encryption is nothing but requesting the time server to extend the file access time for already expired file. In this proposed model, we mainly try to show the importance of the time enabled function as this is a very new primitive that was still not yet implemented in EHR. The implementation of the time controlled function has been highlighted. The data owner who wants to upload a file into the cloud server will initially try to upload the files into the cloud server with a basic privilege of one day access i.e ., twenty four hours as default access time for all the files. If any data user or patient who want to access the file after the stipulated date and time, then the data owner should send a request for the proxy server to enable the timer for the expired files[12].

For example, if the proxy server re-encryption technique is taken in the form of a example : Initially the data owner uploads a file into the cloud server with a default access time of twenty four hours, the file can be accessed for all the data users within the stipulated time period. Now if the file access permission got expired in the EHR storage area, then the data owner request the proxy server to enable the re-encryption facility ,in which he want the file access for some more days from that expired date. Now the proxy will click on re-encryption button that was available in his login for the owner requested file. Here the re-encryption is one form of acknowledgement that is given for the time server to update the time seal. So once the time server receives the request from proxy server, the time server will try to update the file access permission again for some more days as requested by the proxy server. So that within this time period all the data delegates can access the files from the electronic health storage server.

The time seal is one form of a trapdoor for an effective time period and concealed by the private key of the time server. In the re-encryption operation, the proxy server will encapsulate the effective time into the re-encrypted ciphertext. In order to reduce computing cost, the proxy server will not re-encrypt

the ciphertext until they are accessed, which is so called lazy re-encryption mechanism [13]. In the query phase, the data owner can conduct ordinary search operations with his own private key. However, the delegatee has to generate a keywords trapdoor with the help of the time seal. The cloud data server will not return the matched files unless the effective time encapsulated in the time seal accords with the time in the re-encrypted ciphertext, which is different from traditional proxy re-encryption SE schemes.

#### IV. MATHEMATICAL REPRESENTATION OF OUR PROPOSED NRE-dtPECK MODEL

In this section we mainly discuss about the mathematical representation of our proposed NRE-dtPECK model. Now let us look about that in detail as follows:

First we can find the notations that are used in our current mathematical model.

**TABLE I - List of mathematical notations**

Notation	Description
$\theta$	Delegation indicator
$GP$	Global parameter
$sk_S, pk_S$	Private and public keys of data server
$sk_{TS}, pk_{TS}$	Private and public keys of time server
$sk_R, pk_R$	Private and public keys of user
$R_i, R_j$	Delegator and Delegatee
$W, Q$	Keyword set
$S_T$	Time seal: trapdoor of effective time
$C_i (C_j)$	Ciphertext for delegator (delegatee)
$T_{Q,i} (T_{Q,j})$	Trapdoor of delegator (delegatee) on $Q$

The proposed NRE-dtPECK scheme consists of following algorithms with an indicator  $\theta$ . When its value is 1, the delegation function will be activated. Otherwise, the proxy re-encryption will not be enabled. Now let us discuss about each of them in detail as follows:

**Global Setup (k)** Here the global parameter is represented with a notation like GP, where this will contain a security parameter k for identifying the input.

**KeyGenSer (GP)** Here the keyGenSer is mainly used for generating a pair of keys like public key and private key contained in a single pair ( $sk_S, pk_S$ ) [14] for the EHR data server or data center.

**KeyGenRec(GP)** Here the global parameter GP is taken into account as input parameter and then this function is mainly used for generating a private and public key pair ( $sk_R, pk_R$ ) for the receiver.

**KeyGenT S(GP)** Here the global parameter GP is taken into account as input parameter and try to generate the pair wise keys for time server with a pair like ( $sk_{TS}, pk_{TS}$ )[15].

**dPECK(GP,  $pk_S, pk_{Ri}, sk_{Ri}, W$ )** Here  $GP, pk_S, pk_{Ri}, sk_{Ri}$  and a keyword set  $W = (w_1, \dots, w_l)$  are taken as the inputs, the function returns a ciphertext  $CI$  of  $W$  for  $Ri$ .

**Trapdoor(GP,  $pk_S, sk_{Ri}, Q$ )** Here  $GP, pk_S, sk_{Ri}$  and a keyword query for  $Q = (w_1, \dots, w_m), m \leq l$  are taken as the inputs, it outputs a trapdoor  $TQ, I$  for  $Q$  generated by  $Ri$ .

**Test (GP, TQ, I, skS, CI )** Taking GP, TQ,I , skS and a ciphertext CI of Was the inputs, the function returns '1',if W includes Q and '0' otherwise.

## **V. METHODOLOGY**

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage the application is divided into a number of modules and then coded for deployment. The proposed concept has been implemented on Java programming language with JEE as the chosen language in order to show the performance this proposed multi keyword ranked based search over encrypted cloud data. A Real Cloud Service provider called as DRIVEHQ Cloud Service provider is used in this application. This cloud service provider will provide a space up to 1 GB for storing the files which is used by the application. The application is divided mainly into following five modules. Now let us discuss about these modules in short as follows:

### **Data Owner Module**

Here the data owner is one who has the facility to upload all the sensitive information of patient health information into EHR storage server. For uploading the data he need to register first into the account with all his credentials and then try to login into the account with those login credentials. Here the data owner has the facility of uploading the file into the EHR with initial level of encryption and then he also has the facility to access the files at any time within the stipulated time period. Also he has the facility to request the proxy server for re-encryption of expired file.

### **Data User Module**

Here the data user is one who has the facility to search for various files which are available in the EHR storage server. Once if he found any file is available in the server database, then immediately he will send a request for the data owner to provide key access for accessing the file in a plain text manner. Once the file request is approved by the data owner for the corresponding file of the data user, then only the file can be accessed in a plain text manner , if not data user cant able to access his file at any cost. Also the data user has the facility to request the files from corresponding data owner if the files are expired in the storage server.

### **Conjunctive Keyword Search Module**

As we all know that with the single keyword search we can search the files with only one keyword, the conjunctive keyword search function provides the users more convenience to return the accurate results that fulfills users multiple requirements at a time . The users do not have to query an individual keyword and rely on an intersection calculation to obtain what they needs. There is no existing proxy re-encryption searchable encryption scheme that could provide the conjunctive keywords search capability without requiring a random oracle. This scheme has solved this open problem. The scheme could provide both the conjunctive keywords search and the delegation function. Unfortunately, it is proved in the random oracle (R.O.) model, which greatly impairs the security level.

## Proxy Re-Encryption Module

In this module ,the proxy re-encryption technology is mainly used for enabling the permission for the time server to extend the time for the expired files from the server database. It will greatly facilitate patient to search any files even the access is blocked for some files in the storage server. This is the first time to include such a benefit in the current EHR storage servers for providing more security for the sensitive data.

## Time Controlled Revocation Module

An important design goal is to enable time controlled access right revocation. The delegation appointment will terminate when the preset effective time period disagrees with the current time. It should prevent the authorized user from accessing the records overtime.

## VI. RESULTS

In this section the performance analysis of our proposed model is considered mainly in terms of security level , efficiency and the utility function to evaluate whether the proposed scheme is suitable for the privacy-preserving in the EHR cloud storage. The proposed NRE-dtPECK will be compared with other relevant schemes according to these indicators. A simulation result on an experimental test-bed is also provided to measure the performance of NRE-dtPECK scheme.

**TABLE II - FEATURES COMPARISON WITH RELATED SCHEMES**

S.No.	SCHEME	F1	F2	F3	F4	F5	F6	F7	F8
1	CP-ABE	NO	NO	NO	NO	NO	NO	YES	YES
2	KP-ABE	NO	NO	YES	NO	---	NO	YES	YES
3	FIELD KEYWORD SEARCH	NO	YES	YES	NO	YES	NO	YES	YES
4	RANGE QUERIES SEARCH	NO	YES	NO	NO	NO	NO	YES	YES
5	SUB-SET KEYWORD SEARCH	NO	YES	NO	NO	NO	NO	YES	YES
6	PROXY RE-ENCRYPTION	NO	NO	NO	YES	NO	NO	YES	YES
7	SECURE ANONYMOUS RE-ENCRYPTION SEARCH	NO	NO	NO	YES	NO	NO	YES	YES
8	RANDOM ORACLE METHODOLOGY	NO	NO	YES	NO	NO	NO	YES	YES
9	PUBLIC KEY SEARCHABLE ENCRYPTION	NO	NO	YES	NO	---	NO	YES	YES
10	NRE-dtPECK	YES	YES	YES	YES	YES	NO	YES	YES

Here the functions are termed as F1, F2, F3 and so on till F8 which is denoted as follows:

F1 = Time Control Function	F4=Proxy Search	F7= No Key Sharing
F2=Conjunctive Keywords Function	F5=Standard Model	F8=Dynamic Data Change
F3=Again KG Attack Function	F6=Boolean Query	

Analysis from Table II infers that first scheme works well for no key sharing and also when data changes dynamically. Second scheme gives good results for keyword guessing attacks, no key sharing and dynamic data changes. Third scheme is accessible for conjunctive keywords, keyword guess attacks, no key sharing, dynamic data change and it also works in standard model. Fourth scheme works well for conjunctive keyword search, no key sharing and dynamic data change functions. Fifth scheme gives good results for conjunctive keyword search, no key sharing and dynamic data change functions. Sixth scheme is accessible for proxy search, no key sharing and dynamic data change functions. Seventh scheme is accurate in functioning for proxy search, no key sharing and dynamic data change functions. Eighth scheme works well for keyword guessing attack function, no key sharing and dynamic data change. Ninth scheme gives good results for keyword guessing attack, no key sharing and dynamic data change functions. NRE-dtPECK(tenth scheme) gives perfect results for time control function which doesnot work well with other schemes. Time controlled access of the files by users enhances the security of files. This scheme is accurate for other functions also like conjunctive keyword function, keyword guess attack function, proxy search, standard model, no key sharing and dynamic data change.

## VII. CONCLUSION

In this proposed paper, a secure, efficient and dynamic search scheme is proposed, which supports not only the storage of patients EHR but also gives the facility of restricting the files from un-authorized users. This novel conjunctive keyword search with designated tester and timing enabled proxy re-encryption function (Re-dtPECK), which is a kind of a time-dependent SE scheme. It could enable the patients to operate their records for a certain limited time period for searching the record. In this application we can restrict the time period based on each and every individual file and the user based. Moreover, the user could be automatically depreciated their access and access priority after a specified period of effective time. In this paper, high level of security for the medical or health records has been given by encrypting the data before it is stored inside the server and also the security can be provided by limiting the access for certain period of time so that, the user cant able to use the same access for a long period of time. By conducting various experiments on this proposed model a conclusion can be made that this is the first time to implement such a Re-dtPECK method into the cloud for providing security for the sensitive data which is to be stored into the cloud in a secure manner.

## VIII. REFERENCES

- [1] "Bloomberg Business: Health Care Technology". Retrieved 12 March 2015.
- [2] "Boston Globe: Web health records firm expands to Boston". Retrieved 12 March 2015.
- [3] "Yahoo? Finance: Care Cloud Concludes 2014. Archived from the original on 22 April 2015. Retrieved 12 March 2015.
- [4] Microsoft. Microsoft HealthVault. [Online]. Available: <http://www.healthvault.com>, accessed May 1, 2015.

- [5] Google Inc. Google Health. [Online]. Available: <https://www.google.com/health>, accessed Jan. 1, 2013.
- [6] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc.4th Theory Cryptogr. Conf., vol. 4392.Amsterdam, The Netherlands, Feb. 2007, pp.535- 554.
- [7] B. Zhang and F. Zhang, "An efficient public key encryption with conjunctive-subset keywords search," J. Netw. Comput. Appl., vol. 34,no. 1, pp. 262–267, 2011.
- [8] J. W. Byun and D. H. Lee, "On a security model of conjunctive keyword search over encrypted relational database," J. Syst. Softw., vol. 84, no. 8,pp. 1364–1372, 2011.
- [9] K. Emura, A. Miyaji, and K. Omote, "A timed-release proxy re-encryption scheme," IEICE Trans. Fundam. Electron., Commun.Comput. Sci., vol. 94, no. 8, pp. 1682–1695, 2011.
- [10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258,pp. 355–370, Feb. 2014.
- [11] W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," Chin. J. Electron., vol. 23, no. 4, pp. 778–782,Oct. 2014.
- [12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007,pp. 321–334.
- [13] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. 14th ACM Conf. Comput. Commun. Secur., Oct. 2007,pp. 456–465.
- [14] J. Li, Y. Shi, and Y. Zhang, "Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage," Int. J. Commun. Syst., doi:10.1002/dac.2942, 2015.
- [15] B. Lynn. The PBC Library. [Online]. Available: <http://crypto.stanford.edu/pbc/>, accessed May 1, 2015.

## IX. ABOUT THE AUTHORS



**DURGAVAJJALA PRATHIMA** is currently pursuing her 2 Years M.Tech in Department of Computer Science and System Engineering at Andhra University College of Engineering, Visakhapatnam, Andhra Pradesh, India. Her area of interests includes Data Mining and Cloud Computing.



**DR. KUNJAM NAGESWARA RAO** is currently working as a Associate Professor in Department of Computer Science and System Engineering at Andhra University College of Engineering, Visakhapatnam, Andhra Pradesh, India. He has more than 15 years of teaching experience. His research interest includes Data Mining and Cloud Computing.