International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Security Framework for Cloud Computing using Fragmentation and Homomorphic Encryption

Savita A., Vasanth

Abstract: ***An invention of cloud computing technology comes with numerous benefits for IT industries and others. The data store in the cloud can be easily shared among stakeholders irrespective of their location, i.e. data availability is very good. Nowadays organizations are switching to cloud platform for storing and sharing data in a decentralized manner. This is significantly reduces the economically burden to the organization. As the data are accessible through network, so major concern is to maintain the data confidentiality. Data breach in any form organization losses their trustworthy, and this affect the reputation of the organization. This is very important to maintain the privacy and security of data all the time. There are so many works has been proposed by many researchers to secure data in the cloud by using various encryption techniques. In this paper, we proposed a security mechanism to maintain confidentiality of data. This method is combination of multiplicative homomorphic encryption algorithms along with vertical fragmentation of data. We have tested our scheme based on crypto delays, communication delays, and query processing delays with an existing work. The results obtained show that our method out-perform the existing work. The results obtained show improvement with the proposed method.***

Index-Terms: ***Security, homomorphic-encryption, cloud-computing, fragmentation, delay.***

I.INTRODUCTION

Nowadays Cloud-Computing [2] is one of the most burning area where many research work is going on. Specially, IT industries exploited this technological advancement as a next generation computing environment. [7] Day by day enterprises realizes the real usages of cloud computing and demand by clients, this is highly expected that the demand of this technology in increase in coming days. The solution provided to client side is cost effective and may be in future cloud computing delivered of more and more cost effective services. Through, this technology data is available as when required by clients. Further, adhering cloud computing industries achieves great benefits economically, because this reduces the overall expenditure cost, operational cost and improves flexibility in the system. There are still some many challenges to be solved for better performance of the cloud environment. The data or information is one of the most crucial thing for clients in this environment. All the operations are performed on the data, so protection and privacy must be preserved in all means with high level vigilance. Therefore, Data-Security in the cloud environment is apex issue, otherwise cloud computing never be successful.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Savita A. Harkude*, Associate Professor, Department of ETE, Sir MVIT, Bangalore (Karnataka) India. E-mail: harkudesavita@gmail.com
Dr. Vasanth G., HOD, Department of CSE, Government Engineering College, Mandya (Karnataka) India. E-mail: gvasanth_ss@yahoo.com.in

The Cloud-Computing, is an emerging technology of computing environment in I-T industries due to its robust efficiency, low deployment cost, high level of availability and accessibility, on-demand and other advantages [4].
In cloud environment [7] security issue should be improved by using well known cryptography algorithms, bio-metrics etc. This is very essential that Cloud Service Providers safeguard security and privacy of personal data of their customers and these things are not compromised at any stage.
In this paper, we have proposed a combination of multiplicative homomorphic-encryption algorithm along with vertical fragmentation of data to improve database confidentiality. This framework distributed the fragmented relations into various sites in an encrypted form. In fig.1. Show the Architecture for multi-region fragmentation of data. In this architecture, [1] public-clouds are consisting of a master-cloud and number of associate regions-clouds. A master-cloud keeps an encrypted replica of the entire data-base or relation, single public-clouds store fragmented parts of the relation [1].

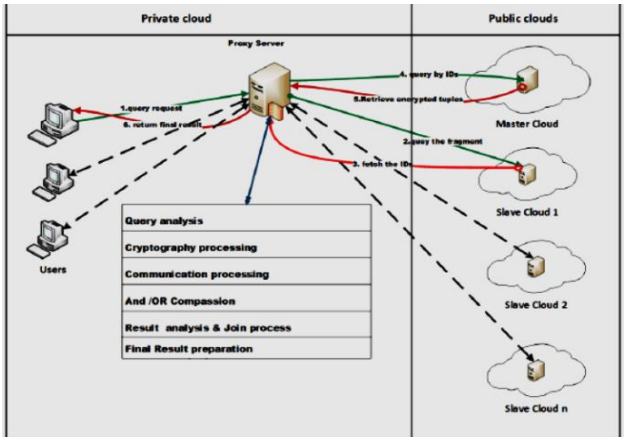

Fig 1- Architecture for multi-region fragmentation [1]

The paper is segregated as follows:
Section-1, consists of a brief introduction of Cloud Computing.
Section-2, literature on various security issues related to cloud computing and various security structure exists along with encryption algorithms are discussed. The proposed security frame work is discussed in Section-3.
Section-4, shows the experimental results and discussions. Finally, the paper is concluded with future work in the section-5.

II.RELATED WORKS

There are so many works has been done on the security issue in cloud computing. But there is always a scope of improvements in the existing work.

To have designed a framework to achieve robustness in security mechanism in cloud computing.

There are enormous security frameworks proposed for cloud computing that uses various encryption techniques by various authors. Here, we have discussed few of them.

In [2] authors addressed challenges associates with cloud computing, like security and trust issues. As the clients data transferred to Cloud and thus leaves privacy and protection of user data. The trustworthy factor is very important as cloud computing moves databases. This databases are always vulnerable and attract security attacks. Today's scenario there are endless security attacks exist. So, cope up with these attacks needs proper security mechanism while transferring data in decentralized manner in the cloud. So, data should always be encrypted when placed in certain sites.

In [3] authors have discussed few security threats in protection of privacy and techniques to cope up these issues. Generally, cryptography methods are uses to achieve high level of privacy and protect data stored, processed, accessed and audited in the cloud through a secure channel. So, every operation in the cloud needs strong support of security. Here, authors have shown double-encryption approach to declare the privacy preserving public cloud data-auditing system. Further, efficient handling of multiple auditing tasks accomplished with help of online signature to support into a multi-user setting. The data encrypted twice and stored in the cloud server.

In this paper [4] authors, proposed a security mechanism using Double-Encryption technique for securely uses data in the cloud. Generally, with the help of double-encryption technique solves key-escrow problems and the Data-Reveal problem with the help of RSA-algorithm of asymmetric-key approaches [4]. In existing m-CLPKE technique suffer from Certificate-less Encryption and single-level encryption. This encryption technique helps in achieving highly secured data and sharing it to in cloud environment.

In this paper [5] authors addressed data security issue of cloud computing. Cloud computing facilitates data sharing in a distributed manner along with other resources and services. As these data are accessed through network in an open environment always make it vulnerable to security threat. The Rijndael method is implemented and explain the security issues associated with encrypted data. To achieve confidentiality of data, storing data in double encrypted.

In this paper[6] proposed RSA algorithm based double layer encryption to achieve high level of security and trust worthy of the data. This scheme resolves key-escrow difficulty and the data exposed problem by the help of RSA-algorithm of public key cryptography-approach. The major advantage of double layer encryption technique is to provide user to highly secure data. This helps in achieving security & privacy of the data.

In paper [7] authors discussed various methods of security mechanisms for cloud computing. The data security based on biometrics, cryptography, public key for Cloud Computing discussed. Finally, the paper focused on the security mechanism improvement by combining cryptography and biometrics.

In this paper [8] authors designed double encryption method using RSA. The escrow-problem and Data-Reveal problem by RSA algorithm of asymmetric-key approach is well discussed.

In [9] authors have discussed cross-virtual machine side channel attacks on cloud computing. This attack is a common attack in cloud by exploiting the correlation between multiple virtual machines on a same hardware. The authors have proposed secure double encryption standard (SDES-384bit) as a mitigation technique to side channel attacks.

In this paper [10] an improve security mechanism is derived for data access in the cloud computing for organization like bank location by using location-based encryption. This method is very useful for many applications for banks, institutions and many more.

In this paper [11] authors uses RC6 algorithm and proposed an improved component to guaranteeing information security mechanism guarantee privacy and integrity of data stored in the cloud. The results clearly indicate that data are secure at a good level of resistance against the threats and attacks.

In this paper [12] authors focuses to optimize and specify the user encryption-processing especially for sensitive-data. Here, also they proposed double encryption technology. Further enhancement in data transport in safe and effective manner is achieved by incorporating check of messages technology with double encryption. The client creates symmetric-key and message-digest, and set them sum behind the message encrypted transmission together. It secures that the user data be security and integrity. It used the double-encryption technology to encrypt symmetric-key once again, which secures the security of key-transmission.

In this paper [13] authors discussed various challenges and open issue using re-encryption scheme in outsourced cloud data. Basically, the data confidentiality issues are well discussed. This paper obtained the restrictions of choosing appropriate encryption-algorithm to connect secure re-encryption scheme in cloud data services.

In this paper [14] a novel Homomorphic Encryption method is proposed for cloud computing security. The following Homomorphic-Encryption cryptosystems namely RSA, Paillier, El-Gamal, Goldwasser-Micali, Boneh-Goh-Nissim and Gentry on Cloud-Computing Platform has discussed. The following parameters are used for comparison Homomorphic-Encryption type, Privacy of data, Security applied to and keys used.

In this paper [15] is mainly focused on security issues in today's cloud computing environment. Many cryptographic techniques used for data secure it, secure sharing of data with authenticated clients are well discussed.

In this paper, authors discusses about existing decryption scheme for protecting data-privacy in cloud-data service. Terms to identify the exact encryption-algorithm to create decryption scheme. It takes decryption as the research components, which are independent of encryption-algorithms.

III.METHODOLOGY

In this section, discussed methodology and associated algorithm. The overall methodology is comprises of two different phases are data fragmentation and encryption algorithm. Before transferring data, data firstly vertically fragmented and these data are encrypted and store in the cloud.

We have used multiplicative homomorphic encryption algorithm, since it can encrypt data without private key.

Fragmentation: Vertical Fragmentation method: The fragmentation of data is three different types are vertical, horizontal and hybrid. In our design we have chosen vertical fragmentation, because it increases the performance of transaction. The projection operation is performed on a relation and it divided into sub-relations according to a subset of attributes of the relation.

Encryption: The Homomorphic encryption [14] is used on the data transferred to cloud for improve the security of storage data and secure operations of those data. The advantage of doing this is to protect the client interest and improve the trustworthy of the system. But at last, data decryption is necessary at each operation. Client may require to show the secret key to server (Cloud provider) for decryption of data before evaluation of required calculations, which maybe disturb the confidentiality and privacy of data stored in Cloud. As per implementation, we proposed an application of method to execute functions on encrypted-data without decrypting, which will provide the same results after calculations as if we have worked directly on the raw-data.

Homomorphic Encryption systems are performed to do operations on encrypted-data without the knowledge of secret key (without decryption); the client is the only holder of the secret key. When we decrypt the result of any operation, it is the same as if we had carried out the calculation on the raw data.

Encryption is homomorphic, if: from Enc(a) and Enc(b) it can be possible to evaluate Enc(f (a, b)), where f can be: +, ×, ⊕ and without using the secret key. Among the Homomorphic-encryption, we distinguish, as per the operations that allow to access on raw-data, the additive Homomorphic-encryption is only additions of the raw-data [14].

- Ek is an encryption algorithm with key k.

- Dk is a decryption algorithm.

Dk (Ek (n) × Ek (m)) = n×m OR Enc (x⊗y) = Enc(x) ⊗Enc(y)

DL (EL (n) × EL (m)) = n+m OR Enc (x⊕y) = Enc(x) ⊗Enc(y)

First property is called additive homomorphic-encryption, and the 2nd is multiplicative homomorphic-encryption. An algorithm is fully homomorphic if both properties are satisfied simultaneously.

The Multiplicative Homomorphic-Encryption (RSA cryptosystem) is used in our analysis.

Let n = pq, where p & q are prime number. Pick a & b such that ab ≡1

(mod ϕ(n). n & b are public while p, q & a are private

$e_k(X)= x^b \bmod n$

$d_k(y)= y^b \bmod n$

Client Company

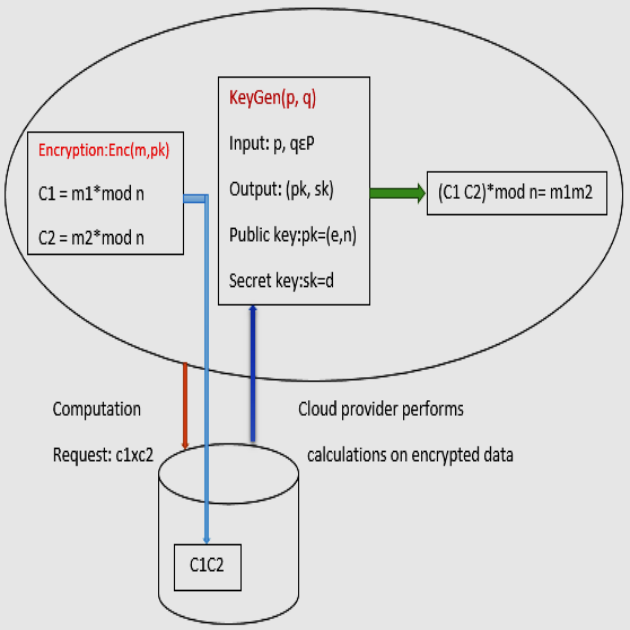

Fig 2: Multiplicative homomorphic encryption applied to cloud data [14].

Phase-I: Data fragmentation:-To achieve the data fragmentation the following operations are needed. The table-I shows the various Notation and symbols used for Vertical fragmentation algorithm. It is a process to access one or more class in database transaction, which can be obtained by dividing transactions. Let C (O) be set of classes accessed by operation.

Type of operations:

a. Extension operation: if C(O) is unitary set i.e. O is directly referencing data from class.
b. Navigation operation: If C(O) has more than one elements.

Transaction- it is composition of queries.

Table-I Notation and symbols used for Vertical fragmentation

Symbol	meaning
D_v	Available data to be fragmented
O_p	Operation Sets
D_k	Column in D_v
E_i	Element in D_k
S_v	Vertical fragmentation Sets

Algorithm 1:
Begin
For each D_k in D_v
For Each O_i in O_p
For each E_i of D_k, i.e accessed by each O_i
If existing link between E_i & E_j
Then value of element + = freq (O_i)
Else
New link between E_i & E_j
Value of this element = freq (O_i)
End If

Let P=empty node set & Q=empty link set & G_p= (P,Q)
Node1 = any element of D_k
P+ = Node1
While D_k Not Part of P
Lk_{ch} = Link with Highest graph extremity
If Lk_{ch} forms a cycle in G_p
Then C_i be Cycle
If C_i is affinity cycle
Then $C_i$is fragment candidate
Else
$C_j$is fragment candidate
End if
$S_v(D_k)$+=C_j
S_v+ = $S_v(D_k)$
Return S_v
end
Step2: All Vertical fragmented sets stored in different locations as S_{v1}, S_{v2} & S_{v3}
Step3: Encryption methodology

Phase –II: Homomorphic encryption

Before transferring fragmented data to the cloud, data are encrypted. The homomorphic encryption algorithm can encrypt without private key. We are using multiplicative homomorphic encryption.
Algorithm 2:

Begin

Let A & B are Plain texts

N_1 = Prime number

N_2 = Prime number

P1 & P2 be constants

$S=N_1N_2$

P1P2= (mod Φ (k)) where k & P2 are public

$P1,N_2,N_1$ are private

Step1: Private key generation

Input = (A, B)

Public key =P_k= (e|, S|)

Private Key = (d |, S|)

Step2: Encryption using RSA

$E_k(X_1) = X^{P1}$ mod S ---------- RSA encryption of X_1

$E_k(X_2) = X^{p1}$ mod S ---------- RSA encryption X_2

Step 3: storing $E_k(X_1)$ and $E_k(X_2)$ At cloud

$E_H = E_k(X_1)*E_k(X_2)$

Step 4: Downloading encrypted data from cloud

Input = (P1,P2)

Keygen (P1,P2)

Public key= P_k= (e|, S|)

Secret Key =C_k= d

Step 5: Decrypting data

$X_1X_2 = (E_H)^d$ mod S

IV.RESULTS AND DISCUSSIONS

The proposed method is the combination of homomorphic encryption and vertical encryption technique and compared with the method discussed in [1], where encryption technique is used along with distribution system. The investigation is carried out for three different queries [1] are (1) Single predicate selection, (2) Two predicate selection with logical function and (3) three predicate selection with multiple logical function. The performance is evaluated of our proposed methodology following three parameter are considered for the result comparison with [1].

(a) Communication delays:

It is time taken to fetch the data from multiple regions of the cloud infrastructure. The similar database query we can see that proposed algorithm takes 20% lesser time to fetch same data.

Table 1:- Showing comparison between earlier method and proposed method.

Query No.	Earlier method	Proposed Method
Query 1	400	320
Query 2	1230	984
Query 3	1690	1510

Below graph showing the comparison between earlier method and proposed method**.**

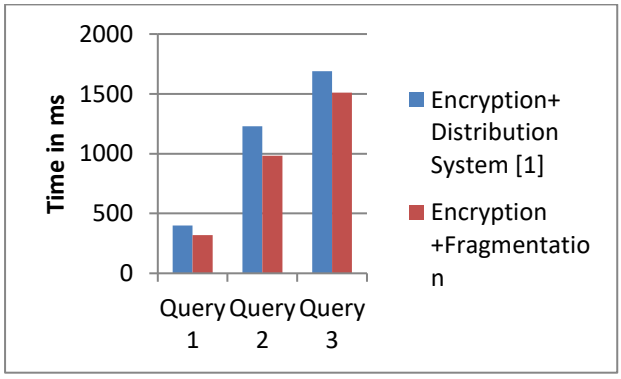

Fig.3 Communication delay analysis.

The fig. 3 shows the communication delays occurs in computing different types of queries for our proposed method and method proposed in [1]. (The model proposed in [1] communication delay is higher as compared to our method.) The communication delays gradually increases from query type-1 to query-3. So, for different types of queries our proposed model encounter lesser delay than the model proposed based on encryption along with distributed system techniques.
(The model proposed in [1] communication delay is higher as compared to our method) can be eliminated.

(b) *Crypto Delays:*

It is time taken to convert plane text data to cipher text and reverse. In this study, we have only considered time for conversion without including communication delay. So we can see that proposed algorithm can process 15% faster than other.

(c)

Table 2:- Crypto delays comparison

Query No.	Earlier method	Proposed Method
Query 1	239	153
Query 2	271	225
Query 3	318	249

Below graph is showing comparison f crypto delay analysis.

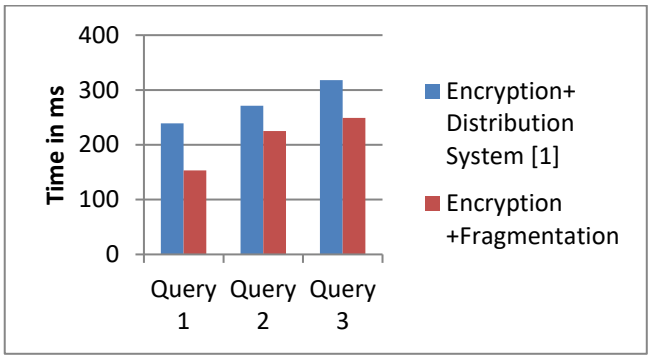

Fig.4 Crypto delay analysis.

Fig. 4 shows the Crypto delays for three types of queries for both the models. The crypto delays are proportionally affected by message size. The crypto delay should always be minimum is preferable. The results obtained show that for different types of queries delay is gradually increases significantly. Our proposed methodology is also encountering a gradual increase in the delay. But the result clearly shows that our proposed method is significantly gives better performance.

(d) Total Query processing delays:It is the overall delay to process a query including communication and decryption delay. We can see that query processing delay is improved by 12% for proposed algorithm**.**

Table 3:- Comparison of previous with new method.

Query Number	***Earlier method***	***Proposed Method***
Query 1	***710***	***528***
Query 2	***1600***	***1407***
Query 3	***2100***	***1830***

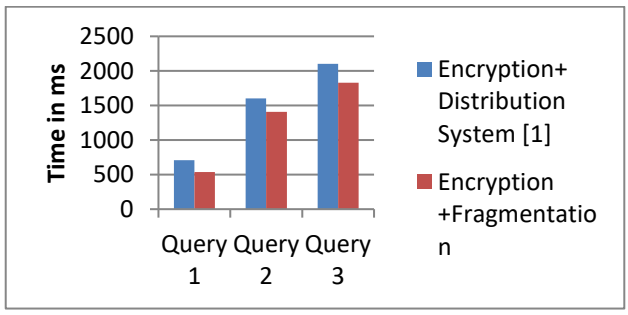

Fig.5 Total Query processing delays analysis.

Fig. 5 shows the query processing delays for different type of queries for our proposed method and method proposed in [1]. The result show that our methodology performs better. For different types of queries query processing delay is increase for both the methods but the method [1] is always achieved higher query processing delay. The results shows better performance comparatively.The overall analysis of the result shows that method proposed by us gives better and reasonable results.

V.CONCLUSION

In this paper, we have proposed a new secure framework for cloud computing environment. The data is stored in different sites of cloud by splitting the original relation with the help of vertical fragmentation technique. The vertical fragmentation helps in minimizing query processing, communication etc. delay. We have also addressed the major challenging issue exists in cloud computing environment is security and privacy of data. The multiplicative homomorphic encryption algorithm is used for protect the privacy of data stored in the cloud and accessed from the cloud. The fragmented and encrypted data is stored in different sites for user access of these data. Our simulation work showing that our method is outperform than existing one compared in the paper.

In future, this framework can be tested by incorporating other encryption techniques to improve the security level.

REFERENCES

1. Amjad Alsirhani et al., “Improving Database Security in Cloud Computing by Fragmentation of Data”, IEEE International Conference on Computer and Applications (ICCA), pp. 43-49, 2017.
2. Geethu Thomas et al., “Cloud computing security using encryption Technique”, 2013, pp.1-6.
3. M.Mahindha et al., “Double Encryption Based Auditing Protocol Using Dynamic Operation in Cloud Storage”, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 3, PP. 294 – 299, 2017.
4. Saisree and Kiran, “Double Encryption for Securely Outsourcing the Data in Cloud”, Macaw International Journal of advanced Research in Computer Science and Engineering (MIJARCSE) , Volume 1, Issue 1, November-2015, pp. 1-5.
5. D.Gayathri and Manjula.A “Double Encryption Using Rijndael Algorithm for Data Security in Cloud Computing”, International Journal of Emerging Technologies in Engineering Research (IJETER) Volume 5, Issue 2, PP.1-3, 2017.
6. D.Usha and M.Subbbulakshmi, “Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud”, International Journal of Scientific & Engineering Research Volume 9, Issue 5, May-2018, PP. 91-98.
7. Yuvraj Gupta, “Enhancing Data Security in Cloud Computing”, International Journal of Scientific & Engineering Research, Volume 3, Issue 12, December-2012.
8. [8] Govindaswamy H R and Bhanu K N, “Implementation Of Privilege Data In Cloud Computing By Double Encryption Concept”, International Journal of Advanced Networking & Applications (IJANA) , pp.118-120, 2016.
9. Toa Bi Irie Guy-Cedric and Suchithra R, “Implementation Of A Novel Algorithm Secure Double Encryption Standard (Sdes-384bit) To Prevent Side-Channel Attack For Cloud Data Center”, International Journal of Mechanical Engineering and Technology (IJMET), Volume 9, Issue 9, September 2018, pp. 1118–1126.
10. Goikar Vandana T. et al., “Improve Security Of Data Access In Cloud Computing Using Location”, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.2, February-2015, pg. 331-340.
11. Salim Ali Abbas and Malik Qasim Mohammed, “Improving Data Storage Security in Cloud Computing Using RC6 Algorithm”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. V (Sep.- Oct. 2017), PP 51-56.
12. Chang Xue-zhou, “Network Data Encryption Strategy for Cloud Computing”, Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015, pp.693-697.

13. Lizhi Xiong and Zhengquan Xu, "RE-Encryption Security Model Over Outsourced Cloud Data", International Conference on Information and Network Security (ICINS 2013),2013,pp.1-5.
14. Deepanshi Nanda, and Sonia Sharma, "Security in Cloud Computing using Cryptographic Techniques", IJCST Vol. 8, Issue 2, April - June 2017.

AUTHORS PROFILE

Mrs. Savita A. Harkude, obtained B.E in ECEand M.E from PDA College of Engineering, Gulburga University in 1999 and pursuing Ph.D under VTU. Currently working as Associate Professor in MVIT, Bangalore.Her research is centered on Communication system, network security.

Dr. Vasanth G., B.E, M.E, and Ph.D, Professor and HOD, Dept. Of Computer Science Engineering, Government Engineering College, K R Pet, Mandya, Karnataka. He has having 23 years of teaching and 10 years of research experience. He is an AICTE expert committee member. His research interest in network security and computer programming.