A SECURE MULTIOWNER DYNAMIC GROUPS DATA SHARING IN CLOUD

Sawase Akanksha and B.M.Patil
P.G. Dept., MBES College of Engineering Ambajogai, Maharashtra, India

ABSTRACT-
Cloud computing is becoming more interesting day by day. Now it is important to use of cloud services increases therefore to do something for improving efficiency and security of cloud computing. Most of cloud services provided by cloud are non turstable. Security vulnerability of online storage systems is one of the non trustable. To solve this problem a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. This scheme is able to support dynamic groups. These dynamic groups are generating a group signature and dynamic broadcast encryption techniques, any cloud user can share data with others securely. The main purpose of this scheme is securely using cloud services storing and sharing by multiple owner groups.

KEYWORDS- *Dynamic groups, cloud computing, data sharing, broadcast encryption*

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.
Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. Basically Cloud computing is broken down into three segments: application, storage and connectivity. Each segment serves a different purpose and offers different products for businesses and individuals around the world. Multi-owner information exchange is a model form sharing business data of large organizations, which allows owners to create, manage and control their information/data in cloud. Cloud storage permits a large number of users having different roles and access permissions to share and store their data [1].
One of the most fundamental services provided by cloud is data storage. Let us consider an example. A company allows its staffs in the same department to store and share data in the cloud. By using the cloud, the staffs can be share local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored data. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential.
To preserve data privacy, [2] a solution is to encrypt data files, and then upload the encrypted data into the cloud. But designing an efficient and secure data sharing scheme for groups in the cloud is have some issues. First, identity privacy is one of the most important issue in a cloud computing. There is no guarantee of identity privacy; users may be unwilling to join in cloud computing systems because their real identities could be easily exposed to cloud providers and attackers [3]. Another thing is traceability. Consider in above company example any misbehaved staff can give others in the company by sharing false data files without being traceable. Therefore, traceability is important to help group manager (e.g., a company manager) to reveal the real identity of a user.

Second is that any member in a group should be satisfied with the data storing and sharing services provided by the cloud, which is called as the multiple-owner manner. In this scheme each user in the group is able to read data, as well as modify his/her part of data in the entire data file which is shared. Another thing is groups are normally dynamic in practice, e.g., if a new staff is participated and in a company. The changes in membership make secure data sharing extremely difficult. On the other hand, the system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with every data owners, and obtain the corresponding decryption keys.

Therefore the proposed system identified the problems in multi owner data sharing scheme and proposed an efficient protocols and cryptographic techniques for solving problems in the traditional approach. In this proposed scheme signature key is generating and by using these key data owners can encrypt the all files. Suppose new user register into group the users need not to contact the data owner during the downloading of files.

II. LITERATURE SURVEY

Plutus is [4] a cryptographic storage system that enables secure files sharing without trusting on the file servers. Plutus features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. The mechanisms in Plutus is to reduce the number of cryptographic keys exchanged between users by using filegroups, distinguish file read and write access, handle user revocation efficiently, and allow an untrusted server to authorize file writes. Plutus achieves strong security with overhead comparable to systems that encrypt all network traffic.

SiRiUS [5] assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction.

B. Wang, B. Li, and H. Li, [6] Knox, a privacy-preserving auditing scheme for shared data with large groups in the cloud. They utilize group signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity of the signer on each block. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group.

Goyal, et al [7] develop a new cryptosystem for One-grained sharing of encrypted data that call Key-Policy Attribute-Based Encryption (KP-ABE). In cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KPABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a ciphertext if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryptions and user secret key update to cloud servers.

Ateniese et al leveraged [8] proxy reencryptions to secure distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks. The primary advantage of this scheme is that they are unidirectional. The drawback of this system is that it provides only a limited amount of trust is placed in the proxy.

Lu et al proposed [9] a secure provenance scheme, which is built upon group signatures and ciphertext-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs

encrypted data with her group signature key for privacy preserving and traceability. However, user revocation is not supported in their scheme.

III. SYSTEM MODEL AND SCHEME DESCRIPTION

3.1 system model

System model consists of three entities: the cloud, a group manager and a no of group members as shown in fig 1 .The users are not fully trusted on cloud. But the cloud server will not delete or modify user data which is stored on cloud due to various security techniques. Group manager takes charge of system parameters, user registration, user revocation and revealing the real identity of a dispute data owner. Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group.

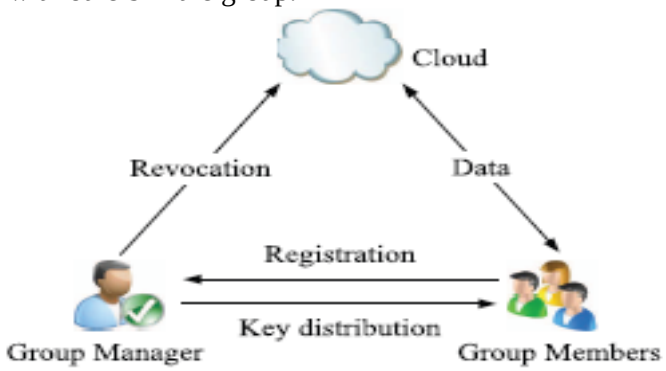

Fig 1 System Model

3.2 Scheme Description

Bilinear Map

Let G_1 and G_2be an additive cyclic group and a multiplicative cyclic group of the same prime order q, respectively [11]. Let e:$G_1 * G_1 \rightarrow G_2$ denote a bilinear map constructed with the following properties:
1. Bilinear: For all a, b ϵZ_q^* and P, Q ϵ G_1,e (aP, bQ)=e$(P,Q)^{ab}$.
2. Nondegenerate: There exists a point P such that e(P,P)≠ 1.
3. Computable: There is an efficient algorithm to compute e (P,Q) for any P,QϵG_1.

A) System Initialization

Generating a bilinear map group system S= (q,$G_1, G_2, e(.\ ,\ .)$).
Selecting two random elements H,$H_0 \in G_1$ along with two random numbers $\varepsilon_1, \varepsilon_2 \epsilon Z_q^*$ and computing U=$\varepsilon_1^{-1} H$ and $V = \varepsilon_2^{-1} H \epsilon G_1$such that$\varepsilon_1 . U = \varepsilon_2 . V = H$. the group manager Computes
$H_1 = \varepsilon_1 H_0$ and $H_2 = \varepsilon_2 H_0 \epsilon G_1$.
Randomly choosing two elements P,G ϵG_1 and a number $\gamma \epsilon Z_q^*$, and computing W=$\gamma . P, Y = \gamma . G$
And Z=e(G,P) respectively.
Publishing the system parameters including ($S, P, H, H_0, H_1, H_2, U, V, W, Y, Z, f, f_1, Enc(\ )$),where f is a one-way hash function: .$\{0,1\}^* \rightarrow Z_q^*$; f_1 is hash function: secure.$\{0,1\}^* \rightarrow G_1$; And Enck () is a secure symmetric encryption algorithm with secret key k .In the end, the parameter $(\gamma, \varepsilon_1, \varepsilon_2, G)$ will be kept secret as the master key of the group manager. After the registration of user i with identity ID, the group manager selects numbers$x_i \epsilon Z_q^*$ and computes A_i and B_i Then adds (A_i, x_i, ID_i) and user gets private key.

B) Cloud

Create a local Cloud and provide abundant storage services. The users can up-load their data in the cloud. We develop this module, where the cloud storage can be made secure. By using cloud user can share data to each other.

C) Group Member

Group members are a set of registered users that will Store their private data into the cloud server and Share them with others in the group. After successful connection of cloud users should have to

register with their personal details like name password, email id, etc.Once the registration completes admin send the signature key after preserving identity privacy.

D) Group Manager

Group manager takes charge of System parameters generation, User registration, User revocation, and revealing the real identity of a dispute data owner. The Group manager is the admin. The group manager has the records of each and every process in the cloud that is when and which users upload and download data. Also the user belongs to which group etc. The group manager is re-sponsible for user registration and also user revocation.

E) File Security

Encrypting the data file and File stored in the cloud can be deleted by either the group manager or the data owner. It means that the files stored on cloud are encrypted form. File can be deleted by user who have file signature key. And this key should have only to data owners as well as group manager[12].

F) Group Signature

In a group signature key allows any member of the group to sign messages while keeping the identity secret from verifiers. Another side the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

F) User Revocation

User revocation is performed by the group manager through a public available revocation list (RL), based on which group members can confidentiality against the revoked users. It means that if user is revoked then can't access to it. The system maintains revocation list for each attribute. Revocation is the process of deletion of user[13].

IV. ALGORITHM USED

Algorithms used in this scheme are as follows

1. Signature Generation
2. Signature Verification
3. Revocation Verification

Algorithm (1) Signature Generation

Input: Private key (A, x), system parameters (P, U, V, H, W) and data M

Output: Generate a valid group signature

Begin

Select random numbers $\alpha, \beta, \gamma_{\alpha}, \gamma_{\beta}, \gamma_{x}, \gamma_{\delta 1}, \gamma_{\delta 2}, \in z_q^*$

Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$

Compute the following values

$T_1 = \alpha . U$

$T_2 = \beta . V$

$T_3 = A_i + (\alpha + \beta) . H$

$R_1 = \gamma_{\alpha} . U$

$R_2 = \gamma_{\beta} . V$

$R3 = e(T_{3,}, P)^{\gamma_x} e(H, W)^{-\gamma_{\alpha} - \gamma_{\beta}} e(H, P)^{-\gamma_{\delta 1} - \gamma_{\delta 2}}$

$R_4 = \gamma_x . T_1 - \gamma_{\delta 1} . U$

$R_5 = \gamma_x . T_2 - \gamma_{\delta 2} . V$

Set

c=f (M,$T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5$)

Construct the following numbers

$s_a = \gamma_{\alpha}$+cα

$s_{\beta} = \gamma_{\beta} + c\beta$

$s_x = \gamma_x + cx$

$s_{\delta 1} = \gamma_{\delta 1} + c\delta_1$

$s_{\delta 2} = \gamma_{\delta 2} + c\delta_2$

Return $\sigma = \left(T_1, T_2, T_3, c, s_a, s_{\beta}, s_x, s_{\delta 1}, s_{\delta 2}\right)$

End

Algorithm (2) Signature Verification
Input: System parameter (P, U, V, H, W), M and signature $\sigma = (T_1, T_2, T_3, c, s_a, s_\beta, s_x, s_{\delta 1}, s_{\delta 2})$
Output: True or False
Begin
Compute the following values
$\check{R}_1 = s_\alpha . U - c . T_1$
$\check{R}_2 = s_\beta . V - c . T_2$
$\check{R}_3 = (e(T_{3,}, W) e(P, P))^c \ \ e(T_3, P)^{\delta_x} \qquad e(H, W)^{-s_\alpha - s_\beta} e(H, P)^{s_{\delta 1} - s_{\delta 2}}$
$\check{R}_4 = s_x . T_1 - s_{\delta 1} . U$
$\check{R}_5 = s_x . T_2 - s_{\delta 2} . V$
If c=f (M,$T_1, T_2, T_3, \check{R}_1, \check{R}_2, \check{R}_3, \check{R}_4, \check{R}_5$)
Return True
Else
Return False
End

Algorithm (3) Revocation Verification
Input: System parameter (H_0, H_1, H_2), a group signatureσ, and a set of revocation key $A_1 \ldots \ldots A_r$
Output: Valid or Invalid
Begin
Set temp=e (T_1, H_1)$e(T_2, H_2)$
For i=1 to n
If e $(T_3 - A_i, H_0) = temp$
Return Valid
End if
End for
Return Invalid
End

V. RESULT ANALYSIS

Following are result generated from our scheme. AS in result fig 2 and 3 shows the time required for uploading and downloading the file. To upload a file filesize is taken in kb and time is in minutes.
For uploading and downloading file as the file size increased the time required for both will increased.But time required for uploading is somehow more than downloading file.
The fig 4 and 5 shows generation and accessing 1 MB file.for generating and accessing 1MB file considering 10 users and computation cost requried for it. In fig 4 as the no of users increased the computaion cost of client side remains constant.But for accessing 1MB as the no of users increased the computing cost also increased.The time and computation cost are imporatant parameters in the system to give correct result.

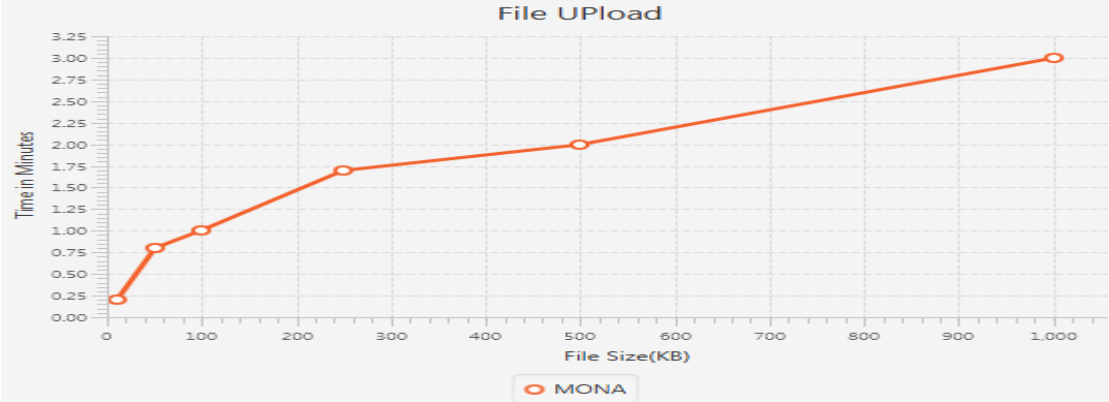

Fig 2. File Upload(file size vs time)

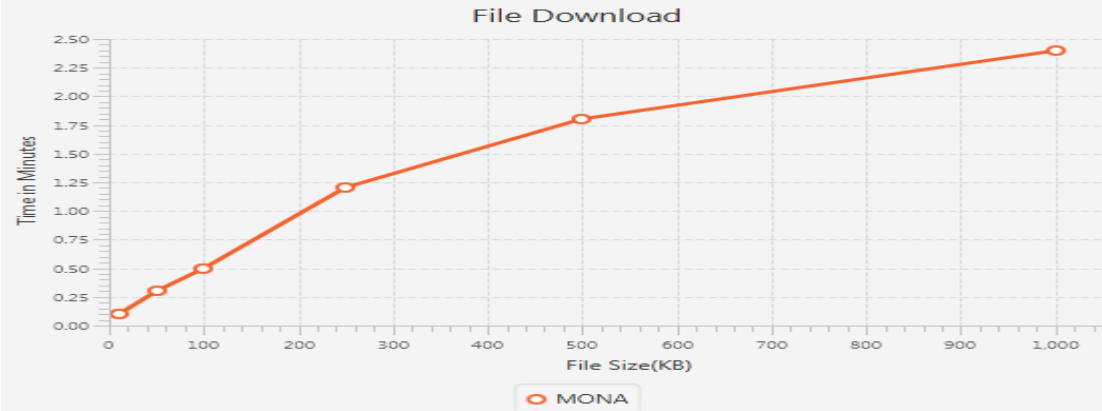

Fig 3. File Download(file size vs time)

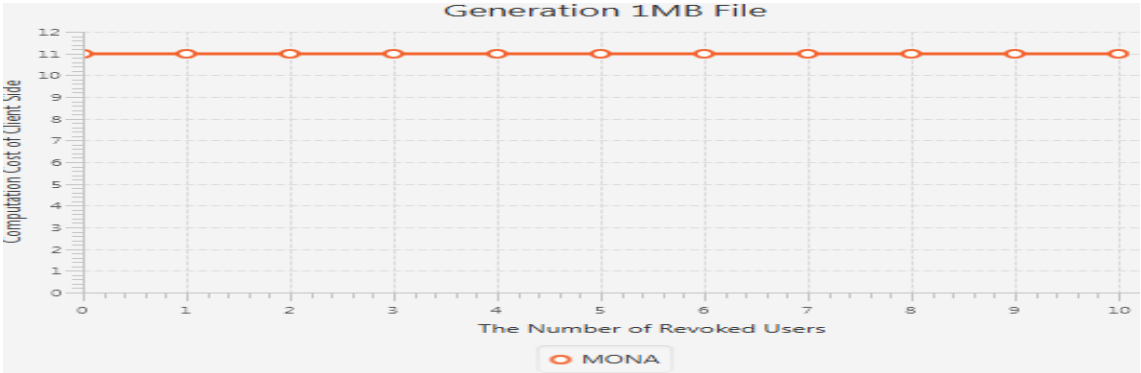

Fig 4 Generating 1MB file(no of user Vs computaion cost)

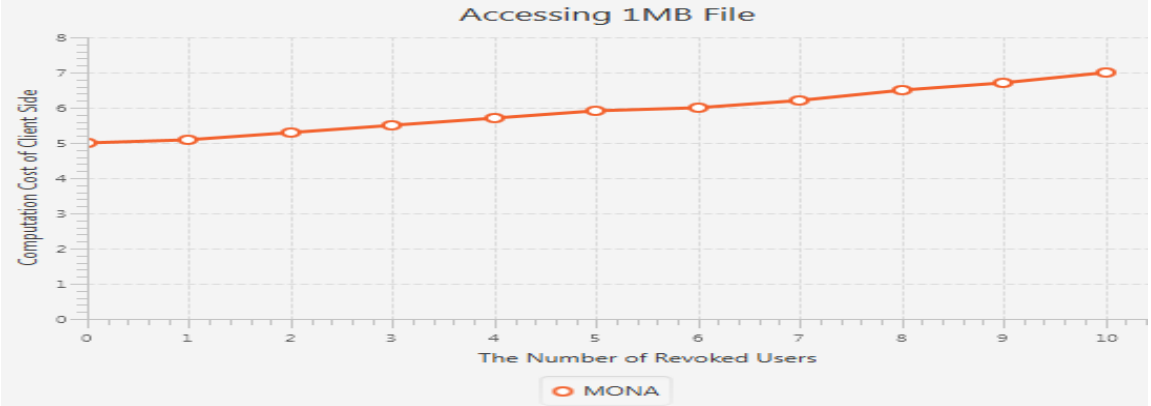

Fig 5 Accessing 1MB file (no of user Vs computaion cost)

VI. CONCLUSION AND FUTURE WORK

In this work a Multiowner secure data sharing in untrusted cloud and solving problem of identity privacy.In this system efficient user revocation can be achieved by using public revocation list without updating a private key of remaining users and new users directly decrypt files stored in cloud. In case of future work in this system only one group manager if in any condition group manager fails then another back up group manager will be there.

REFERENCES

[1] Cloud computing-An Overview by Torry Harris Business solutions pp.1-6, Nov 2013.
[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.
[3] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.
[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131- 145, 2003.
[6] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006
[8] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.D.
[10] Naor, M. Naor, and J.B. Lotspiech, "Revocation and TracingSchemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.
[12] S.Santosh, K.Madhubabu,"Data Security For Multiowner in cloud by using Cryptography Technique Vol.no.02 Issue 04 august 2014.
[13] V.Ajaykumar,Dr.V.Ananadam,"Sharing the secure data in cloud for Multiuser group",vol.no.03,august 2015.

AUTHORS

Sawase Akanksha presently working P.G. student at the Department of Computer Science & Engineering in MBES College of Engineering, Ambajogai, India. She completed her Bachelor's degree in Computer Science & Engineering Department from Aditya Engineering College Beed under Dr. B.A.M. University, Aurangabad, India. She is pursuing her Master's Degree from the College of Engineering, Ambajogai. Her areas of research interest include Computer Networks &Cloud computing

B.M. Patil is currently working as a Professor in P.G. Computer Science & Engineering Department in M.B.E. Society's College of Engineering, Ambajogai, India. He received his Bachelor's degree in Computer Engineering from Gulbarga University in 1993, MTech Software Engineering from Mysore University in 1999, and PhD Degree from Indian Institute of Technology, Roorkee, 2011. He has authored several papers in various international journals and conferences of repute. His current research interests include data mining, medical decision support systems, intrusion detection, cloud computing, artificial intelligence, artificial neural network, wireless network and network security