Public Integrity Auditing for Dynamic Data Sharing with Multi User Modification

Mrs. A. Kumuda #1, Ms. A. Harika #2, Ms. Ch. Anjani #3,
Ms. Ch. Baby Gayathri #4, Ms. M. Tejaswini #5 & Ms. Sk. Haseena #6

#1 Assistant Professor, Dept Of CSE, Qis Institute of Technology, Ongole, Prakasam (Dt)
#2 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)
#3 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)
#4 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)
#5 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)
#6 Student, Dept Of IT, Qis Institute of Technology, Ongole, Prakasam (Dt)

ABSTRACT:

The arrival of cloud computing technology makes the storage outsourcing become a growing trend, which encourages the secure remote data auditing. Data auditing is the process of conducting a data review to measure how company's data is fit for agreed function. This engages profiling of data and assesses the collision of pitiable quality data on the organization's performance and profits. In recent times, some research believes the problem of secure with efficient public data integrity auditing for unified dynamic data. On the other hand, these systems are still not secure beside the collusion of cloud storage server as well as revoked group users during user revocation in practical cloud storage system. In this paper, we found out that the collusion attack in the exiting scheme .An efficient public integrity auditing scheme with secure group user revocation based on vector commitment plus verifier-local revocation group signature. We invented a concrete scheme. We propose a new structure called Decrypt key, which provides efficiency and reliability assurance for convergent key management on mutually user along with cloud storage sides. The design is to apply de-duplication to the convergent keys to influence secret sharing techniques. In particular, we build secret shares for the convergent keys and share out them across multiple independent key servers. Our proposed system rigging the public checking and efficient user revocation, as well as also some fine assets, such as confidently, efficiency, count ability and traceability.

KEYWORDS:

Key management, Insider attacks, Outsider attacks, Data confidentiality, Integrity Checking

I INTRODUCTION Cloud Storage service are such as simple storage services in online data backup services of amazon, and practical cloud based software google drive, dropbox, mozy, bitcasa and memopal have been built for cloud application. There is

invalid result in cloud server such as server hardware, software failure, human maintenance and malicious attack. Rabin data dispersion scheme implemented for practical application and overcome above challenges. Author in [10], [11], [12], [18] provide solutions to integrity and availability of remote cloud store. This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. . Dynamic scheme means when scheme support data modification only data owner cloud modify data. The limited dynamic scheme cloud only efficiently supports special field operation (eg. Append). The static scheme not supports data modification. In publicly verifiable, data integrity check can be performed by data owner and by any third party auditor. Multiple user in group need to share source code they need to access, modify compile and run the shared source code at any time and place. Remote data auditing is only data owner can update its data. Ring signature supports multiple user data operation. The proxy re-signature is private and authenticated channels exist between each pair of entities. Till today is no solution for above problem in public integrity auditing with group user modification. Real Time Example: In an Group file sharing environment if an user wishes to revocate from a group then the complexity added to the files shared by that user where someone else in the group need to take authority over their files by downloading and reassigning key to that file. In order to overcome that we appoint an third person where his work is to monitor the files of the revocated user and reassign it to someone else in the group based on owners priority without any over head of download. Here we generate private and public key based on the prime no. The main aim of this paper is to search for private and public files. In case of public files users can modify their files and update to it.

II RELATED WORK

Group signatures without revocation. The provably coalition-resistant scalable group signature was described by Ateniese, Camenisch, Joye and Tsudik in 2000 [7]. At that time, the security of group signatures was not totally understood and proper security de_nitions were given later on by Bellare, Micciancio and Warinschi [9] (BMW) whose model captures all the requirements of group signatures in three properties. In (a relaxation of) this model, Boneh, Boyen and Shacham [16] obtained a construction in the random oracle model [10] with signatures shorter than 200 bytes [13]. In the BMW model, the population of users is frozen after the setup phase beyond which no new member can be added. Dynamic group signatures were independently formalized by Kiayias and Yung [4] and Bellare-Shi-Zhang [11]. In these models, pairing-based schemes with relatively short signatures were put forth in [5]. Ateniese et al. [6] also gave a construction without random oracles using interactive assumptions. In the BMW model [9], Boyen and Waters independently came

up with a di_erent standard model proposal [19] using more classical assumptions and they subsequently re_ned their scheme [21] to o btain constant-size signatures. In the dynamic model [11], Groth [8] described a system with constantsize signatures without random oracles but this scheme was rather a feasibility result than an e_cient construction. Later on, Groth gave [9] a fairly e_cient realization { with signatures consisting of about 50 group elements { in the standard model with the strongest anonymity level. Revocation. In group signatures, membership revocation has received much attention in the last decade [2, 8, 9, 18] since revocation is central to digital signature schemes. One simple solution is to generate a new group public key and deliver a new signing key to each unrevoked member. However, in large groups, it may be inconvenient to change the public key and send a new secret to signers after they joined the group. An alternative approach taken by Bresson and Stern [22] is to have the signer prove that his membership certi_cate does not appear in a public list or revoked certi_cates. Unfortunately, the signer's workload and the size of signatures grow with the number of expelled users. Song [5] presented an approach handling revocation in forward-secure group signatures. However, veri_cation takes linear time in the number of excluded users. Using accumulators1 [12], Camenisch and Lysyanskaya [9] proposed a method (notably followed by [6]) to revoke users in the ACJT group signature [7] while keeping O(1) costs for signing and verifying. While elegant, this approach is history-dependent and requires users to keep track of all changes in the population of the group: at each modi_cation of the accumulator value, unrevoked users need to update their membership certi_cates before signing new messages, which may require O(r) exponentiations { if r is the number of revoked users { in the worst case. Brickell [3] suggested the notion of veri_er-local revocation group signatures, which was formalized by Boneh and Shacham [1] and further studied in [5]. In their systems, revocation messages are only sent to veri_ers (making the signing algorithm independent of the number of revocations). The group manager maintains a revocation list (RL) which is used by veri_ers to make sure that signatures were not generated by a revoked member. The RL contains a token for each revoked user and the veri_cation algorithm has to verify signatures w.r.t. each token (a similar revocation mechanism is used in [4]). As a result, the veri_cation cost is inevitably linear in the number of expelled users. More recently, Nakanishi, Fuji, Hira and Funabiki [9] described a construction with constant complexities for signing/verifying and where group members never have to update their credentials. On the other hand, their proposal has the disadvantage of linear-size group public keys (in the maximal number N of users), although a tweak allows reducing the size to O(N1=2). In the context of anonymous credentials, Tsang et al. [8, 9] showed how to blacklist users without compromising their anonymity or involving a trusted third party. Their protocols either have linear proving complexity in the number of revocations or rely on accumulators (which may be problematic for our purposes).

Camenisch, Kohlweiss and Soriente [2] suggested handling revocations by periodically updating user's credentials in which a speci_c attribute indicates a validity period. While useful in certain applications of anonymous credentials, in group signatures, their technique would place quite a burden on the group manager who would have to generate updates for each unrevoked individual credential. Paragraphs must be indented. All paragraphs must be justified, i.e. both leftjustified and right-justified. A. Text Font of Entire Document The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes. Recommended font sizes are shown in Table 1. B. Title and Author Details Title must be in 20 pt Regular font. Author name must be in 10 pt Regular font. Author affiliation must be in 10 pt Italic. Email address must be in 9 pt Courier Regular font.

III LITERATURE SURVEY

Micael O Rabin[1]-Proficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. An Information Dispersal Algorithm (IDA) is made that breaks a document F of length L = (F (into n number of pieces F, 1 5 i 5 n), each of length (F, 1 = L/m)), so that every m pieces accomplishment for reproducing F. Dispersal and redoing are computationally beneficial. The entire of the lengths is (F, 1 is (n/m) of L). Since (n/m) can be chosen to be close to IDA, the IDA is space proficient. IDA has different applications to secure and trustworthy limit of information in PC frameworks and even on single circles, to accuse tolerant and viable transmission of data in frameworks, and to exchanges between processors in parallel PCs. For the given issue provably time-productive and exceedingly accuse tolerant indicating towards the n-3D shape is expert, using just uniform size backings.

Giuseppe Ateniese[2][3][4]-Provable Data Possession at Untrusted Stores. Here the author has presented a model for provable data possession (PDP) that allows a user or client that has stored away data or information at a non-trusted server to make sure that the server has the initial information without having the client or user to take the load of recovering the original data. The model which has been proposed, creates multiple possible outcomes and its evidences of ownership by examining non-uniform arrangements of fragments from the server, which confirmly reduces the I/O costs. The client or user keeps up a unified count of metadata to declare the results. The test/response tradition transmits somewhat, relent less measure of data, which limits framework correspondence. Thus, the PDP show the results for the remote document or information evaluation for a large amount of information set in most part speed limit. The author, shows two provably secure PDP arranges that are more viable than past plans, despite when differentiated and plots that finish weaker confirmations. Actually, the overhead at the server is low or also can be uniform, rather than directly going for the area of facts or research, our execution confirms the reasoning of PDP and reveals that the execution of PDP is barriered by the plate I/O and thus not by the cryptographic computation.

Ari Juels [5][6]-Proofs of retrieve ability for Large Files. Characterize and investigate proofs of retrieve ability (PORs). A POR plan empowers a file or back-up service (provider) to create a succinct evidence that a client (verifier) can recover an objective document F, that will be, that the file holds and dependably transmits record information adequate for the client to recoup F completely. A POR may be seen as a sort of cryptographic proof of knowledge (POK), however one uncommonly intended to handle an extensive document (or bit string) F. The Investigation of POR conventions here in which the correspondence expenses, number of memory gets to for the provider, and capacity necessities of the client (verifier) are little parameters basically free of the length of F. Not with-standing proposing new, common sense POR developments, investigate usage contemplations and enhancements that bear on already investigated, related plans. In a POR, dissimilar to a POK, neither the provider nor the verifier need really have information of F. PORs offer ascent to another and surprising security definition who‟s detailing is another commitment of the work. Seeing the PORs as an essential instrument for semi-trusted online documents. Existing cryptographic strategies clients some assistance with ensuring the protection and honesty of documents they recover. It is additionally normal, then again, for clients to need to confirm that don't erase or change documents before recovery. The objective of a POR is to fulfil these checks without clients downloading the records themselves.

YevgeniyDodis[5][7]-Verifications of Retrieve capacity by means of Hardness Amplification, Proofs of Retrieve capacity (PoR), exhibited by Juels and Kaliski[5], allow the client to store F (which is the document) on an untrusted server, and later run a beneficial audit tradition in which the server shows that in any case it has the client's data. Advancements of PoR arrangements attempt to limit the client and server stockpiling, the correspondence multifaceted nature of a survey, and even the amount of archive pieces got to by the server in the midst of the audit. YevgeniyDodis[4] work, there recognize a couple of extraordinary varieties of the issue, illustration:- restricted utilize versus unbounded-utilize, learning soundness versus information soundness, and giving practically perfect PoR anticipates each of these varieties. The improvements either upgrade or whole up the prior PoR advancements, or give the main known PoR arranges with the required properties. In particular, formally exhibit the security of a (propelled) variety of the restricted utilize plan of Juels and Kaliski[5], without making any enhancing assumptions on the lead of the enemy. Build the at first unbounded-utilize PoR arrange for where the correspondence disperse quality is straight in the security parameter and which does not rely on upon Random Oracles, deciding an open question of Sachem and Waters. Gather at first constrained utilize arrange with information theoretic security. The essential comprehension of the work starts from a fundamental relationship between PoR arranges and the possibility of hardness heightening, extensively considered in

disperse quality speculation. In particular, changes start from first abstracting a just information theoretic thought of PoR codes, and after that building practically perfect PoR codes using front line instruments from coding and unpredictability hypothesis.

C. Chris Erway[8][9]-Consider the issue of capably showing the uprightness of data set away at untrusted servers. In the provable information ownership or PDP show, the client pre-forms the data and subsequently sends it to an untrusted server for limit, while keeping a little measure of metadata. The client later demands that the server show that the set away data has not been disturbed or eradicated. The primary PDP arrange applies just two static records. Presentation of a definitional structure and gainful improvements for element provable information ownership or DPDP, which extends the PDP model to support provable overhauls to secure data.C. Chris Erway[9] use another adjustment of accommodated word references in perspective of rank information. The cost of component upgrades is an execution change from (O(1) to O(log n)) (or O(n log n)), for a record including n squares, while keeping up a similar probability of inconvenience making distinguishing proof. The tests exhibit that this log stick is low. Additionally, moreover show to apply the DPDP plan to outsourced record systems and shape control structures.

IV PROPOSED SYSTEM

The main aim is to provide a new CP-ABE, Policy Management, Key Management and access control for assured deletion for files that are hosted by cloud storage services. We associate files with file access policies that control how files can be accessed. We then present policy-based file assured deletion, in which files are assuredly deleted and made unrecoverable by anyone when their associated file access policies are revoked. We describe the essential operations on cryptographic keys so as to achieve access control and assured deletion. Policy-based deletion will be useful Secure of file assured deletion and File permanently inaccessible based on policies each file associated with data key Each data key associated with control key all control keys maintained by key manager.

We describe the essential operations on cryptographic keys so as to achieve access control and assured deletion. File assured deletion is also leverages existing cryptographic techniques, including attribute-based encryption(ABE) and a quorum of key managers based on threshold secret sharing.

- Here, we extend the existing definitions and also removed the drawbacks with that system and introduced a secure data transfer in the network. And also it will protects the data lose and also data thefts.
- It also having secure messaging module which protects the user's message from other persons in the network.

Advantages

- Highly secured data transfer with advanced encryption technique the other person cannot decrypt it easily.

- Here we used Attribute Based Encryption system which provides more security for our data.
- The receiver can send multiple key requests to the data owner for the single data.
- The new system provides ABE with outsourced decryption: verifiability. This verifiability used guarantees that a user can efficiently check if the transformation is done correctly.
- **Confidentiality**: It using pairing, the proposed method makes it difficult for a malicious third party to decrypt communication contents, even if they eavesdrop on communications between the client and the server.
- **Search speed**: The user can check whether a document contains keywords by perform single pairing calculations, which increase the searching speed.
- **Traffic efficiency**: Keyword search and re-encryption requires only one round of communication, and provides efficiency.

V Implementation

Data Owner Module

The Cloud data owner is the entity that originates file data to be stored on the cloud as based condition of attributes and policies given the data owner. All the transaction of the user in data uploading, only to key manager to security purpose. A set of Keys are only to be generated by attribute based on key manager.

Data owner operation are following they are

- User Registration
- Login
- Data Key Generation
- Control Key Generation
- File upload
- File download
- Change key

Key Manager Module

The key manager or key authority maintains the set of policy-based of users and their data keys and control keys that are used to encrypt and decrypt data keys. This module provides key generation activities to the data owner's requests by performing encryption, decryption, renewal and revocation to the control keys. Access key basic operation for data outsourcing files upload, download, policy renewal response for client request.

Types of keys:

- Data Key
- Control key
- Access key

Cloud Server Module

The cloud administrator maintains all the user policies as clouds are in a pay-as-you-go manner. Cloud admin is having right to provide user permission to access data performance. Cloud admin provide cloud storage space used in data

storage whose interact to cloud storage. Policy Management and File assured deletion is built on the thin-cloud interface, and assumes only the basic cloud operations for uploading and downloading data files. Cloud admin provide different types of policies as request of clients.

Policy Management Module

Data owner authorized to access only files whose associated with policies, Unauthorized users does not access to any transaction, Reliable data transaction between key manager and data client and reliable store data in cloud storage. Data Consumer Module The Cloud data Consumer is the entity that originates f ile data to be stored on the cloud as based condition of user attributes and policies given the data owner. All the transaction of the user in data uploading, encrypting, key generating and data sharing communication only to key manager to security purpose.

VI Conclusion:

The older process which were used for the verification of data bases and its secure storage like the division of a document file into „F“ fragments (as proposed by Micael O Rabin[1]) and then finding its perfect length and storing it on a system or server has proven to be efficient but, also ,there need to be certain efficient upgrades to improve the security and maintain reliability of the system. Thus, certain new and improved relevant upgrades are to be done in the proposed scheme. Thus to solve the problem of proper verifiable outsourcing of the information. So, to overcome this deficiency which not only the Micael O Rabin has but, also the other theories, there appears the need to design a new variable of the given authors like the Jules-Kaliski which Ari Jules used for his proof giving in his paper, proposing an system which helps in making available lower storage overhead, also bears with high error rates and can probably be considered as secure related to many relevant circumstances. The scheme to be implemented in Java where the algorithms are to be encoded, knowing that the usefulness of the algorithms are to be implemented. The schemes like vector commitment and AGKA with revoked group user are going to take the method of data integrity of remote data. We will be using different algorithms like MD5 and AES for encryption of important data in our system. The group user uses the AGKA protocol to encrypt/decrypt the given document, where there will be surety that a user in the group will be able to encrypt/decrypt a message from any other group users. The text is going to be a cipher text and the text won“t be directly stored on the server but the mediator will take part in this scheme to upload the ciphered text or document on the server and reproduce it whenever the user needs to retrieve it.

VII References

1. M. Rabin, Efficient dispersal of information for security, Journal of

the ACM (JACM), vol. 36(2), pp. 335348, Apr. 1989.

2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, Provable data possession at untrusted stores, in Proc. Of ACM CCS, Virginia, USA, Oct. 2007, pp. 598609.
3.]G. Ateniese, D. Song, and G. Tsudik, "Quasi-efficient revocation in group signatures," in Proc. of FC 2002, Soughamption, Bermuda, Mar. 2002, pp. 183–197.
4. G. Ateniese, R. Burns, Provable data possession at untrusted stores. Cryptology ePrint archive, May 2007. Report 2007/202.
5. A. Juels and B. S. Kaliski. PORs: Proofs of retrievability for large files. Cryptology ePrint archive, June 2007. Report 2007/243.
6. J. Yuan and S. Yu, Proofs of retrievability with public verifiability and constant communication cost in cloud, in Proc. of International Workshop on Security in Cloud Computing, Hangzhou, China, May 2013, pp. 1926.
7. Y. Dodis, S. Vadhan, and D. Wichs, Proofs of retrievability via hardness amplification, in Proc. of TCC 2009, CA, USA,Mar. 2009, pp. 109127.
8. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, Dynamic provable data possession, in Proc. of ACM CCS, Illinois, USA, Nov. 2009, pp. 213222.
9. E. Shi, E. Stefanov, and C. Papamanthou, Practical dynamic proofs of retrievability, in Proc. of ACM CCS 2013, Berlin, Germany, Nov. 2013, pp. 325336.
10. G.R. Blakley and C. Meadows, ''Security of Ramp Schemes,'' inProc. Adv. CRYPTO, vol. 196, Lecture Notes in Computer Science,G.R. Blakley and D. Chaum, Eds., 1985, pp. 242-268.
11. A.T. Clements, I. Ahmad, M. Vilayannur, and J. Li, ''Decentralized Deduplication in San Cluster File Systems,'' in Proc.USENIX ATC, 2009.
12. J.R. Douceur, A. Adya, W.J. Bolosky, D. Simon, and M. Theimer,''Reclaiming Space from Duplicate Files in a Serverless Distributed File System,'' inProc. ICDCS, 2002, pp. 617-624. [9] Dario Catalano, Dario Fiore," Vector Commitments and their Applications", NSF grant CNS-1017471.
13. Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring," Provable Data Possession at Untrusted Stores", October 29– November 2, 2007, Alexandria, Virginia, USA.Copyright 2007 ACM 978-1-59593-703-2/07/0011
14. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg,''Proofs of Ownership in Remote Storage Systems,'' in Proc.ACM Conf. Comput. Commun. Security,Y.Chen,G.Danezis,and V. Shmatikov, Eds., 2011, pp. 491-500
15. D.Harnik, B.Pinkas, A.Shulman-Peleg, ''Side Channels in Cloud Services: Deduplication in Cloud

Storage,''IEEE SecurityPrivacy, vol. 8, no. 6, pp. 40-47, Nov./Dec. 2010.
16. S. Kamara, K. Lauter, ''Cryptographic Cloud Storage,'' in Proc. Financial Cryptography: Workshop Real-Life Cryptograph. Protocols Standardization, 2010, pp. 136-149.
17. M. Li, ''On the Confidentiality of Information Dispersal Algorithms and their Erasure Codes,'' inProc. CoRR, 2012, pp. 1-4abs/1206.4123.
18. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Proofs of retrievability via hardness amplification," in Proc. of ESORICS 2009, Saint-Malo, France, Sep. 2009, pp. 355–370.
19. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. of ACM CCS, Illinois, USA, Nov. 2009, pp. 213–222
20. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp. 525– 533
21. J. Yuan and S. Yu, "Proofs of retrievability with public verifiability and constant communication cost in cloud," in Proc. of International Workshop on Security in Cloud Computing, Hangzhou, China, May 2013, pp. 19–26
22. E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in Proc. of ACM CCS 2013, Berlin, Germany, Nov. 2013, pp. 325–336.
23. Cloud9. (2011) Your development environment, in the cloud. Cloud9. [Online]. Available: https://c9.io/
24. Codeanywhere. (2011) Online code editor. Codeanywhere. [Online]. Available: https://codeanywhere.net/
25. eXo Cloud IDE. (2002) Online code editor. Cloud IDE. [Online]. Available: https://codenvy.com/
26. B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proc. of IEEE CLOUD 2012, Hawaii, USA, Jun. 2012, pp. 295–302.
27. B. Wang, L. Baochun, and L. Hui, "Public auditing for shared data with efficient user revocation in the cloud," in Proc. of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp. 2904–2912.
28. J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121–2129.
29. D. Catalano and D. Fiore, "Vector commitments and their applications," in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.
30. Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," in Proc. of EUROCRYPT 2009, Cologne, Germany, Apr. 2009, pp. 153–170
31. D. Boneh and H. Shacham, "Group signatures with verifierlocal

revocation," in Proc. of ACM CCS, DC, USA, Oct. 2004, pp. 168– 177
32. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proc. of Asiacrypt 2001, Gold Coast, Australia, Dec. 2001, pp. 514–532.
33. D. Boneh and X. Boyen, "Collision-free accumulators and failstop signature schemes without trees," in Proc. of EUROCRYPT 2004, Interlaken, Switzerland, May 2004, pp. 56– 73.

Authors Profile

Mrs A Kumuda, M.Tech., working as an Assistant Professor in the department of Computer Science & Engineering in QIS Institute of Technology, Ongole, Andhra Pradesh, India.

Ms. A Harika pursuing B Tech in the department of Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively.

Ms. Ch Anjani pursuing B Tech in the department of Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively

Ms. Ch Baby Gayathri pursuing B Tech in the department of Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively

Ms. M Tejaswini pursuing B Tech in the department of Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively

Ms. Sk Haseena pursuing B Tech in the department of Information Technology from Qis Institute of Technology, Ponduru Road, Vengamukkalapalem, Ongole, Prakasam Dist, Affiliated to Jawaharlal Nehru Technological University, Kakinada in 2016-20 respectively