# PROTECTED INTRA CONVERSATION INFORMATION CONTROL IN ORGANIZATION

*G.Dineshkumar,S.Kamaraj,L.Krishnakanth*
*UG students*
*Adhiparasakthi Engineering College*

*Mr. K. Chairmadurai*
*Assistant professor*
*Adhiparasakthi Engineering College*

**ABSTRACT--** An organizations an entity comprising multiple people, like an establishment or an association, that features a particular purpose and grouping related functions into manageable units to realize the objectives of the enterprise within the most effective and effective manner. Daily report enables the team manager to have an overview how the team project is progressing in terms of each team member individual tasks without having to talk to each one on a daily basis. In Proposed work, whatever the employee work as a task is automatically create as a PDF file and it will not be rewrite by anyone and daily updating has been updated to the particular file. For accessing the pdf file by team leader, the captcha has been generated to mostly avoid the automatically harvesting the details. If HR Manager wants to see the daily update of the Team Leader, then the QR code has been generated and scanned by them to get access to the file.

## INTRODUCTION

An organization is an entity comprising multiple people, like an establishment or an association, that features a particular purpose andgrouping related functions into manageable units to realize the objectives of the enterprise within the most effective and effective manner. Daily report enables the team manager to have an overview how the team project is progressing in terms of each team member individual tasks without having to talk to each one on a daily basis. In Proposed work, whatever the employee work as a task is automatically create as a PDF file and it will not be rewrite by anyone and daily updating has been updated to the particular file

## PROJECT OBJECTIVE

The main objective of this project is to make the work process easier in organization. Captcha is a way to differentiate between an automated computer program and a human and the main advantages of a QR code is its versatility and can be used anywhere.

## REVIEW OF LITERATURE

***1.Dynamic Secure Group Sharing Framework inPublic Cloud Computing:***
KaipingXue, Member, IEEE, and Peilin Hong, Member, IEEE.

With the popularity of group data sharing in public cloud computing, the privacy and security of group sharing data havebecome two major issues. The cloud provider can't be treated as a trusted third party due to its semi-trust nature, and thusthe traditional security models can't be straightforwardly generalized into cloud based group sharing frameworks. In this paper, wepropose a completely unique secure group sharing framework for public cloud, which may effectively cash in of the Cloud Servershelp buthave no sensitive data being exposed to attackers and the cloud provider.

The framework combines proxy signature, enhanced TGDHand proxy re-encryption together into a protocol. By applying the proxy signature technique, the group leader can effectively grant theprivilege of group management to one or more chosen group members. The enhanced TGDH scheme enables the group to negotiateand update the group key pairs with the assistance of Cloud Servers, which doesn't require all of the group members been online all thetime. By adopting proxy re-encryption, most computationally intensive operations can be delegated to Cloud Servers without disclosingany private information. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfiesthe security requirements for public cloud based secure group sharing.

***2.Public Integrity Auditing for Shared DynamicCloud Data with Group User Revocation:***
Tao Jiang, Xiaofeng Chen, and Jianfeng Ma.

The advent of the cloud computing makes storage outsourcingbecome a rising trend, which promotes the secure remotedata auditing a hot topic that appeared within the research literature.Recently some research consider the problemof secure and efficientpublic data integrity auditing for shared dynamic data. However these schemes are still not

secure against the collusion of cloudstorage server and revoked group users during user revocation inpractical cloud storage system.

In this paper, we find out thecollusion attack within the exiting scheme on the our scheme definition.Our scheme supports the public checking and efficient user revocationand also some nice properties, like confidently, efficiency,countability and traceability of secure group user revocation. Finally,the security and experimental analysis show that, compared with itsrelevant schemes our scheme is additionally secure and efficient.

***3.Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud***

:ShengminXu, Guomin Yang_, Senior Member, IEEE, Yi Mu, Senior Member, IEEE and Robert H. Deng Fellow, IEEE

Cloud computing is an emerging computingparadigm that enables users to store their data into a cloudserver to enjoy scalable and on-demand services. Nevertheless,it also brings many security issues since cloud service providers(CSPs) aren't within the same trusted domain as users. To protectdata privacy against untrusted CSPs, existing solutions applycryptographic methods (e.g., encryption mechanisms) and providedencryption keys only to authorized users. However, sharingcloud data among authorized users at a fine-grained level is stilla challenging issue, especially when handling dynamic user groups. In this paper, we propose a secure and efficient finegrainedaccess control and data sharing scheme for dynamic user groups by

(1) defining and enforcing access policies supported the attributes of the data;

(2) permitting key generation center(KGC) to efficiently update user credentials for dynamic user groups;

(3) allowing some expensive computation tasks to be performed by untrusted CSPs without requiring any delegationkey.

***4.Anonymous and Traceable Group Data Sharing in Cloud Computing:***

Janzen ,Member, IEEE, Tianqi Zhou, Xiaofeng Chen, Senior Member, IEEE

Group data sharing in cloud environments hasbecome a hot topic in recent decades. With the popularityof cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved.In addition, how to achieve both anonymity and traceability isalso a challenge in the cloud for data sharing.

This paper focuseson enabling data sharing and storage for an equivalent group in thecloud with high security and efficiency in an anonymous manner.By leveraging the key agreement and therefore the group signature, a noveltraceable group data sharing scheme is proposed to supportanonymous multiple users in public clouds. On the one hand group members can communicate anonymously with respect tothe group signature, and the real identities of members can betrayed if necessary.

On the other hand, a common conference keyis derived based on the key agreement to enable group membersto share and store their data securely. Note that a symmetricbalanced incomplete block design is employed for key generation,which substantially reduces the burden on members to derivea common conference key. Both theoretical and experimentalanalyses demonstrate that the proposed scheme is secure andefficient for group data sharing in cloud computing.

***5.Spatial Group Sparsely Regularized NonnegativeMatrixFactorization for Hyper spectral Unfixing:***

Xinyu Wang, YanfeiZhong, Senior Member, IEEE, Liangpei Zhang, Senior Member, IEEE, and YanyanXu

In recent years, blind source separation (BSS) hasreceived much attention in the hyper spectral unfixing field dueto the fact that it allows the simultaneous estimation of bothendmembers and fractional abundances. Although great performancescan be obtained by the BSS-based unmixingmethods,the decomposition results are still unstable and sensitive to noise.Motivated by the first law of geography, some recent studies haverevealed that spatial information can lead to an improvement inthe decomposition stability. In this paper, the group-structuredprior information of hyper spectral images is incorporated intothe nonnegative matrix factorization optimization, where thedata are organized into spatial groups. Pixels within a localspatial group are expected to share the same sparse structurein the low-rank matrix (abundance). To fully exploit the groupstructure, image segmentation is introduced to generate thespatial groups. Instead of a predefined group with a regularshape (e.g., a cross or a square window), the spatial groupware adaptively represented by superpixels.

## EXISTING SYSTEM

In existing system, they have to update their daily work and attendance also if they have to send any information means they have to go and inform to their particular HR manager and even the Team Leader have to do the same thing for getting any information or send any information or to update any Employee details to the HR manager and this consumes time and it also delay our works.

## PROPOSED SYSTEM

A modern development in time and technology requires faster information broadcasting. United,

personalized, intelligent information applications are more significant in business and personal lives. In Proposed work, whatever the representative work as an undertaking is consequently make as a PDF record and it won't be rework by anybody and day by day refreshing has been refreshed to the specific document. For getting to the pdf record by group team leader, the captcha has been created to generally keep away from the naturally reaping the subtleties. In the event that HR Manager needs to see the everyday refresh of the Team Leader, at that point the QR code has been generated and examined by them to gain admittance to the document. The attendance has been recorded by the user login. So every time user gets login to their system the particular attendance has been taken.For getting to the pdf record by group team leader, the captcha has been created to generally keep away from the naturally reaping the subtleties. In the event that HR Manager needs to see the everyday refresh of the Team.United, personalized, intelligent information applications are more significant in business and private lives.whatever the representative work as an undertaking is consequently A modern development in time and technology requires faster information broadcasting. United, personalized, intelligent information applications are more significant in business and personal lives. In Proposed work, whatever the representative work as an undertaking is consequently make as a PDF record and it won't be rework by anybody and day by day refreshing has been make as a PDF record and it won't be rework by anybody and day by day refreshing has been refreshed to the specific document.

## SYSTEM ARCHITECTURE:

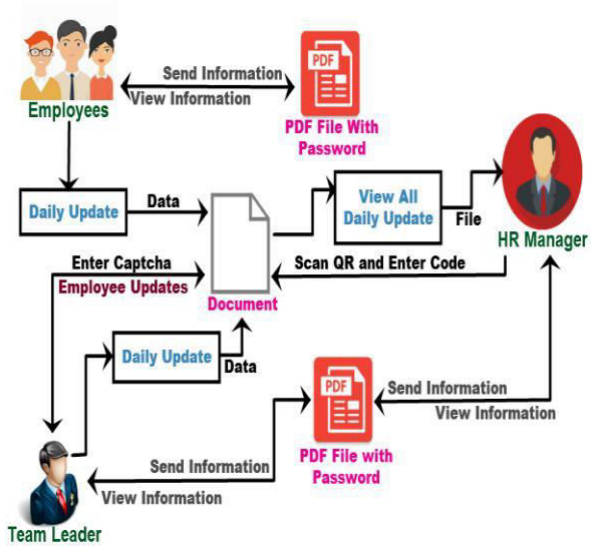


*Fig 4.1 SYSTEM ARCHITECTURE*

## LISTOF MODULE

In these system having the following modules as follows

Authority verification
Daily updating
Captcha and QR code generation
Information sharing
Secure pdf access

## AUTHORITY VERIFICATION

Every time the authentication of the team leader has to be verified by the HR manager in the organization. Whenever employee wants to login or join they have to specify the team leader identity and employee identity, then HR manager will verify the team leader details. If the team leader records found, the employee will be accepted to authenticate.

## DAILY UPDATING

In any organization, the daily updating needs to be done by every employee. The daily report updating is typically a document prepared by employees to submit to their team leader. A daily report updates a team leader or manager about an ongoing project. It should provide an overview that describes each member's tasks and progress. The employee task or work is automatically create as a PDF file and it will not be rewrite by anyone and daily updating has been updated to the particular file

.

## CAPTCHA AND QR CODE GENERATION

Captcha may be a thanks to differentiate between an automatic computer virus and a person's . It has become the most widely used standard security technology to prevent automated computer login. Captcha has been generated for the pdf file, every time the team leader want to access the file they needs to give the captcha. If HR Manager wants to see the daily update of the Team Leader, then the QR code has been generated and scanned by them to get access to the file.It has become the most widely used standard security technology to prevent automated computer login.

## INFORMATION SHARING

If in case of any emergency issues such as any secret information, the employee datas will automatically converted into PDF. The employee can send the secret information to the particular team leader, manager and employee within team. The manager and team leader can also send the information to any employee within organization.Access the file they needs to give the captcha. If HR Manager wants to see the daily update of the Team Leader**.**

## SECURE PDF ACCESS

The PDF file can be accessed by anyone within organization, but to open or read the pdf file, the password authentication will be done. The employee who get the pdf file have to put their login credentials to access it. If someone wants to get the file who is not the particular person whom I want to send, the pdf file could not be accessed by them because of the password authentication.It should provide an overview that describes each member's tasks and progress

## CONCLUSION AND FUTURE ENHANCEMENT

In this generation where everything must be very faster and secured, an leading edge improvement in time and innovation requires quicker data broadcasting. Joined together, customized, astute data applications are increasingly critical in business and personal lives. In every organization where employee allocated with task is commenced when task is automatically transformed into the file which is even secured access by the team leader. during which we also using the captcha to stop from the automated access from the bots and it's even secured accessed by the team leader. eventually when task is completed, the HR manager is meant to done the inspection or verification, the QR code is generated for secure access In Local Area Network, the proposed hybrid encryption mechanism could also be customized for transferring the sensitive data from work station to host based applications. In web based applications, the proposed mechanism enables the transfer of sensitive data from user to user, from user to server and from server to server which are located outside of the organization. during a cloud environment, more number of individuals are accessing the online server locally or globally to share the sensitive data.The proposed hybrid encryption technique is extremely helpful to reinforce the safety for web based transactions in future.innovation requires quicker data broadcasting. Joined together, customized, astute data applications are increasingly critical in business and personal lives. In every organization.from user to server and from server to server which are located outside of the organization.

## REFERENCES

[1] L. Zhou, V. Varadharajan, and M. Hitchens, Cryptographic rolebased access control for secure cloud data storage systems Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 23812395, 2015.

[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, Secure cloud storage meets with secure network coding in IEEE INFOCOM, 2014, pp. 673681.

[3] D. He, S. Zeadally, and L. Wu, Certificateless public auditing scheme for cloud-assisted wireless body area networks, IEEE Systems Journal, pp. 110, 2015.

[4] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on scientific theory , vol. 22, no. 6, pp. 644654, 1976.

[5] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, An efficient rfid authentication protocol providing strong privacy and security Journal of Internet Technology, vol. 17, no. 3, p. 2, 2016.

[6] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, An efficient protocol for authenticated key agreement, Designs Codes and Cryptography, vol. 28, no. 2, pp. 119134, 2010.

[7] X. Yi, Identity-based fault-tolerant conference key agreement, IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 170178, 2004.

[8] R. Barua, R. Dutta, and P. Sarkar, Extending joux protocol to multi party key agreement (extended abstract). Lecture Notes in computing , vol. 2003, pp. 205217, 2003.