Efficient and Secure Group Data Sharing Model Using Cloud Computing

Mohit Kabadi2, Gitesh Ghorpade3, Munot Sarode4, Sameer Sagar5
1Department of Computer Engineering,Pimpri Chinchwad College Of Engineering and Research, Pune 412101 India
2Department of Computer Engineering,Pimpri Chinchwad College Of Engineering and Research, Pune 412101 India
3Department of Computer Engineering,Pimpri Chinchwad College Of Engineering and Research, Pune 412101 India
4Department of Computer Engineering,Pimpri Chinchwad College Of Engineering and Research, Pune 412101 India

Abstract - Traditionally, the purpose of mirrors was to see our reflection in it. But wouldn't it be great if we use current technology of networking world through the medium of the Internet of Things (IoT) in these traditional mirrors. This concept is widely used in smart display devices to showcase interactive multimedia interface [1]. So to have it in these ambient homes as well as in viable regions will make the mirrors smart. This paper provides the design and development of a smart mirror which offers the user with real time information of best current updates of newscast, climate and apparent time equivalent to the distinct locality and scheduled work and meetings. These contents will be displayed on the two ways mirror mounted with LED monitor display in a wooden frame. These basic features will be made available from Internet using Raspberry Pi module for managing on it. By means of the identity verification method we can distinguish the handler's face and validate the handler. This feature can also be used to determine the scheduling of an assignment allocated to handler.
Keywords: **Research, Publication, Papers**

I. INTRODUCTION

In recent times as the concept of cloud computing rises, cloud storage is said to be the one of the hotspots of the storage of information It basically refers to a model, that provides the data storage. Here, CSP (cloud service provider) is directly responsible for making data available as well as accessible according to the requirement of user.0Storage capacity is either bought or leased from provider to store the data by the individual or organization. This service can easily be accessed through the the application, which utilizes the API such as cloud storage gateway

Moreover, in the past few years, it has been observed that the demand of cloud storage has been increased phenomenal in accordance with the use of personal as well as business purpose, since it is highly based on the virtualized infrastructure and much more flexible in terms of multi-tenancy, scalability and availability. 07

Since the cloud, computing provides USA the feature of pay as you go service, the organization needs to pay just for the service they use, and cloud service provides precisely the same. Business exploitation the caesium will truly scale back up to seventy p.c of energy consumption. CSP is completely liable for the upkeep of the info and still because the alternative tasks like shopping for the extra storage capability. Since the backup of the info area unit settled in many places within the globe, it can even be applicable because the proof backup of natural disaster. Meanwhile, cloud storage is one service, that isn't mentioned the physical device, however it's the aggregation of the many server and storage for its users.

II. LITERATURE SURVEY

1.Efficient and Secure Group Data Sharing Model based on Selection scheme in Cloud environment

Description: Cloud computing is aforementioned to be the service oriented computing technology, that area unit reasonable and flexible over the web. In past few years the cloud has become additional matured and provided several services, one of the primary service is knowledge sharing in cluster, wherever the data can be simply shared from one member to another. How-ever, whereas sharing the knowledge security is one of the primary concern. In past many methodology has been projected. However, these ways lacked from the practicableness. Hence in this paper we've propose methodology relies on the selection theme. Here General cluster key's generated and moreover General Key agreement protocol is decentralized based model wherever the knowledge area unit controlled by the owner within identical cluster. Moreover, the projected methodology is evaluated by analysing the comparative analysis based mostly on the numerous range of parameter. Result Analysis suggest that our methodology merely outperforms the existing one.

Keywords: cloud Computing, security, cluster knowledge sharing

2.Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud Description: With info storage and sharing services among the cloud, users will just modify and share info as a bunch. to substantiate shared data integrity are verified publically, users among the cluster got to be compelled to cypher signatures on all the blocks in shared info. fully fully totally different blocks in shared info ar sometimes signed by {different|totally fully fully totally different| completely different} users as a result of info modifications performed by different users. For security reasons, once a user is revoked from the cluster, the blocks that were antecedently signed by this revoked user got to be re-signed by associate degree existing user. The straightforward methodology, that enables associate degree existing user to transfer the corresponding a district of shared info and re-sign it throughout user revocation, is inefficient as a result of the massive size of shared info among the cloud. throughout this paper, we've a bent to propose a completely unique public auditing mechanism for the integrity of shared info with economical user revocation in mind. By utilizing the thought of proxy re-signatures, we've a bent to permit the cloud to re-sign blocks on behalf

Fig.1 : Block Digram

of existing users throughout user revocation, therefore as that existing users haven't have to be compelled to be compelled to transfer and re-sign blocks by themselves. additionally, a public voucher is usually able to audit the integrity of shared info whereas not retrieving the complete info from the cloud, although some a district of shared info has been re-signed by the cloud. Moreover, our mechanism is in associate degree passing position to support batch auditing by verifying multiple auditing tasks at a similar time.

3.NPP: A New Privacy-Aware Public Auditing Scheme for Cloud DataSharing with Group Users

Description: Today, cloud storage becomes one of thecritical services, as a result of users will simply modify and share information with others in cloud. However, the integrity of sharedcloud information is vulnerable to inevitable hardware faults, soft-ware failures or human errors. To guarantee the integrity ofthe shared information, some schemes are designed to allowpublic verifiers (i.e., third party auditors) to expeditiously auditdata integrity while not retrieving the entire users' information fromcloud. Sadly, public auditing on the integrity of shared information could reveal information owners' sensitive informationto the third party auditor. In this paper, we tend to propose afresh privacy-aware public auditing mechanism for sharedcloud information by constructing a homomorphic verifiable groupsignature. Not like the prevailing solutions, our theme requires at least t cluster managers to recover a trace key hand and glove, which eliminates the abuse of single-authority power and provides non frameability. Moreover, our theme ensures that group users will trace information changes through selected binary tree; and will recover the latest correct information block when the current information block is broken. In addition, the formal security analysis and experimental results indicate that our scheme is incontrovertibly secure and economical.

4. Enabling Efficient and Protected Sharing of Data In Cloud Computing

Description: Cloud storage plays a very important role significantly in applications like medical files transfer and inexperienced computing where in-house data storage systems square measure established. In case of group-shared data, the data face every cloud-specific and conventional executive threat. Secure data sharing among a gaggle that counters executive threats of legitimate notwithstanding malicious users is an important analysis issue in cloud. Protected Sharing of knowledge in cloud got to maintain: data confidentiality and integrity; access control; data sharing (forwarding) whereas not victimization computes intensive re-encryption; executive threat security; and forward and backward access management. The PrSDC methodology encrypts a file with one coding key. A pair of wholly completely different key shares for each of the users square measure generated, with the user only getting one share. The Possession of 1 share of a key permits the PrSDC methodology to counter the executive threats and prevents stealing of medical files or simply just in case of inexperienced computing on-line credit payment details. The alternative key share is keep by a sure third party, that's termed the scientific discipline server.

III. EXISTING SYSTEM

In Existing system data is share through the social media, Email, and centralized system but there is no security provided by the system who can recover the data changed by the hacker. In existing system use end to end communication of computers which does not have any security system for data transaction.

IV. PROPOSED SYSTEM

Since the structure and overall arrangement of optical access networks is complicated and meantime, the quantity of operational fiber is big, failures of optical fiber links occur a lot of oftentimes, and thus, the price and operation, administration and maintenance (OAM) stays at a high level. The period on-line fiber-fault detection and site within the optical access network with ancient optical domain reflector (OTDR) is complicated and dear, and has low resolution of the fault location.

•We transfer the data between manager and the employees who are shared data between two systems. When data is upload on system then we are stored in cloud server as well as proxy server for security purpose.

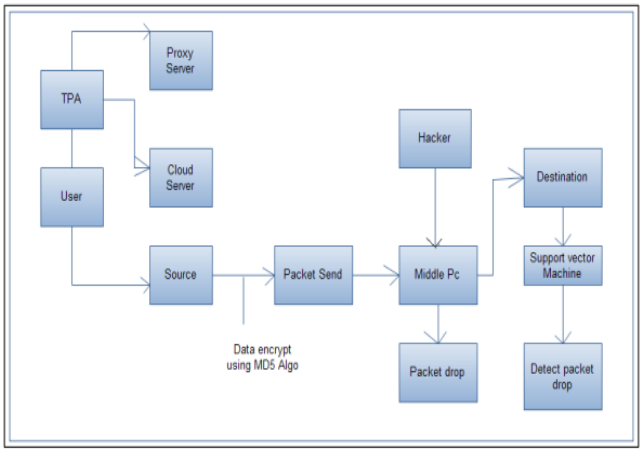
•If hacker change data between transaction then we are traces them and recover data using support vector machine (machine learning algorithm).

Architecture Diagram

So we are securely share and transferred data between multiple users on cloud computing.

Advantages of Proposed System

1) Secure data transaction
2) Data in encrypted through transaction
3) Data store in cloud server
4) Effective and efficient system for data transaction



V. MATH

Input: Employee and manager are share their data on cloud server

Output: Data is transferred securely between employee and manager.

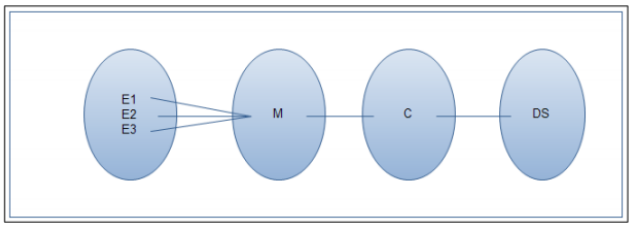


Fig 2: Model

System Description:
Where,
E1= Employee 1, E2= Employee 2, E3=Employee 3, M=Manager, C=Cloud Server, DS=data sharing platform
Objects Involved: Employee, Cloud Server, Manager, Functional relations, Web Security, Data Security, Machine learning, Cloud Computing.
Functions: Functions implemented to get the Manager get all details of Employee data on cloud server.
Success Conditions: Successfully algorithm implementation and proper input.
Failure Conditions: 1. Huge data can lead to more time consumption to get the information. 2. Hardware 3. Software failure.
The space complexity depends on Presentation and visualization of discovered patterns. More the storage of data more is the space complexity
Above mathematical model is NP-Hard.

VI. CONCLUSION

Group data sharing in the cloud plays an eminent role when the data has to be distributed among the others. Moreover, security is one of the big concerns when it comes to preserving the privacy. In this research work, we have developed a methodology based on the selection scheme, which helps in securing the data. We are providing cloud base encryption system for database for security purpose. Data is encrypted during the transaction which never decrypt.

REFERENCES

1. Giuseppe Ace to, Valerie PepsiCo, Antonio Escape, “The role of Information and Communication Technologies in Healthcare: Taxonomies, Perspectives, and Challenges”
2. Rue Zhang and Ling Liu,” Security Models and Requirements for Healthcare Application Clouds”.
3. ANSI, ISO/TS 18308 “Health Informatics-Requirements for an Electronic Health Record Architecture”, ISO 2003.
4. R. Bakker, B. Barber, R. Tervo-Pellikka, A.Treacher, (eds.), “Communicating Health Information in an Insecure World” in:
5. Proceedings of the Helsinki Working Conference. 43:1, 1995. 2.
6. B. Barber, D. Garwood, P. Skerman, In: Security in Hospital Information Systems, Security and data protection programme presented at the IMIA.
7. A. Sonawane, M. U. Inamdar and K. B. Bhangale, "Sound based human emotion recognition using MFCC & multiple SVM," *2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC)*, 2017, pp. 1-4, doi: 10.1109/ICOMICON.2017.8279046
8. Bhangale, Kishor, and K. Mohanaprasad. "Speech Emotion Recognition Using Mel Frequency Log Spectrogram and Deep Convolutional Neural Network." In *Futuristic Communication and Network Technologies*, pp. 241-250. Springer, Singapore, 2022.
9. Bhangale, Kishor Barasu, and K. Mohanaprasad. "A review on speech processing using machine learning paradigm." *International Journal of Speech Technology* 24, no. 2 (2021): 367-388.
10. Bhangale, Kishor & Kothandaraman, Mohanaprasad “Survey of Deep Learning Paradigms for Speech Processing” Wireless Personal Communications. 1-37. 10.1007/s11277-022-09640-y, 2022.
11. Biradar, Priya, Priyanka Kolsure, Sujata Khodaskar, and Kishor B. Bhangale. "IoT based smart bracelet for women security." *Int. J. Res. Appl. Sci. Eng. Technol.(IJRASET)* 8, no. 11 (2020): 688-691.
12. Bhangale, Kishor B., Pranoti Desai, Saloni Banne, and Utkarsh Rajput. "Neural Style Transfer: Reliving art through Artificial Intelligence." In *2022 3rd International Conference for Emerging Technology (INCET)*, pp. 1-6. IEEE, 2022.
13. Sarraf, Rajan, Shalini Ojha, Damini Biraris, and Kishor B. Bhangale. "IoT based smart quality water management system." *International Journal* Of Advance Scientific Research And Engineering Trends5, no. 3 (2020).

14. Mapari, Rahul, Kishor Bhangale, Laukik Deshmukh, Prashant Gode, and Ankit Gaikwad. "Agriculture Protection from Animals Using Smart Scarecrow System." In *Soft Computing for Security Applications*, pp. 539-551. Springer, Singapore, 2022.
15. Anand, Tejveer, Sourabh Upare, Siddhant Jain, Maithili Andhare, and Kishor Bhangale. "Deployment of Real-Time Energy Monitoring System Using IoT." In *2022 3rd International Conference for Emerging Technology (INCET)*, pp. 1-4. IEEE, 2022.
16. Mapari, Rahul G., Kishor B. Bhangale, Pranjal Patil, Harish Tiwari, Shivani Khot, and Sanjana Rane. "An IoT based Automated Hydroponics Farming and Real Time Crop Monitoring." In *2022 2nd International Conference on Intelligent Technologies (CONIT)*, pp. 1-5. IEEE, 2022.
17. Mapari, Rahul G., Harish Tiwari, Kishor B. Bhangale, Nikhil Jagtap, Kunal Gujar, Yash Sarode, and Akash Mahajan. "IOT Based Vertical Farming Using Hydroponics for Spectrum Management & Crop Quality Control." In *2022 2nd International Conference on Intelligent Technologies (CONIT)*, pp. 1-5. IEEE, 2022.