International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Survey on Cloud based Collaboration System

Vishwa Patel[1], Tejaskumar Bhatt[2]

[1]ME Student, Department of computer engineering Sardar Vallabhbhai Institute Of Technology ,Vasad,Gujarat, India

[2]Assistant Professor, Department of computer engineering Sardar Vallabhbhai Institute of Technology ,Vasad, Gujarat, India

ABSTRACT

Due to extensive application of cloud computing and web application, A collaboration technology has become popular. Service like Google Docs, Office 365 allow everyone to access files, allowing multiple authors to collaborate in real time. From a security point of view, they can provide transmission protection through TLS, but cloud service provider can still read the user's confidential data. So we use SecCollab system that provide facilities to user that data should be private while using collaborative editors. This research paper carried out such a way which will secure data and protect the privacy of editors.

Keywords: Collaboration, Security, Confidentiality, Privacy Encryption.

I. INTRODUCTION

For the past decade, Internet and Information Technology has been changing the ease, ease of web, and personal, educational, career, employment, recreation, healthcare, and other social causes for different types of fast growing technology In the last 15 years, the nature of the Internet has been constantly changing from static environment web 1.0 to highly dynamic media and Web 2.0 has a more collaborative environment that helps users run software applications, helps in sharing information and helping to make new services online [1].The Collaborative editing system allows multi-users to edit the shared documents on the Internet. Such systems are appealing to many organizations and users because they can increase productivity, reduce cost, and increase convenience. For example, Collaborative systems can be geographically used to apply virtual teams with different members, working at home, or traveling on the road. The primary challenge for the collaborative editing system allows you to manage stability between different local copies of shared documents and synchronize users in shared documents. [2].

Many products provide document editing suites, which allows their users to easily share the author and their tasks, with automatic backup and access control. Multiple users can edit the same document and view others in real time. Many such applications are web-based interface, there is no need to install anything else than the browser, at least reduces both requirements and hardware requirements. Google popular offerings include Google Drive/Docs, Zoho and Microsoft office 365[3].

Due to SaaS pay-as-you model, select their best support service (service efficiency, value and reliability, etc.) to complete changing business needs. At the same time, the user may need to leave an unfamiliar user interface, learn new user interfaces with a temporary collaboration, on the other hand, cloud service users do not have the same service provider [4].

If the document progresses, even if the entire document has been edited, some parts of it will be edited, and for co-author decrypting from the cipher text and editing the most up-to-date document supporting documents, it is highly recommended for various co-authors to include and edit them. Collaboratively editing a document involves multiple co-authors and results in high frequency of editing action [5].

The current measure for our design, we outline a browser extension for the Google Docs service, working as a malware agent between WebPages and servers, changing demolition and traffic fees, AJAX

(Asynchronous JavaScript and XML) such as Private data is not being transmitted straightaway [6].

II. BACKGROUND

In general, the collaboration is performed as follows: each user's operations (e.g. inserting a new element or deleting existing element at given position) are locally executed in non-blocking manner and then are propagated to other sites in order to be executed on other copies[7]. Both share between multiple clients and one server, real time changes between resources, but they do so by using different methods.

2.1 Operational Transformation

In 1989, Alice and Gibbs established the technology called Operational Transformation. Implementation Changes came from research in the Computer Supported Areas (CSCW) and the collaborative editing sector. Operational Transform resumes operations, treats inconsistencies during operation and guarantee, similar results on all nodes. This work is where the proceedings are done. True real-time application An operational change system can be divided into two layers, changing control algorithms and changing function algorithms alters how the conversion function should be executed, in which concurrent functions are established[8].

The transformation functions, on the other hand, are used to transform concurrent operations. Two types of transformation functions have been proposed: inclusion and exclusion transformations.

Multi-dimensional data structure is used in the basic, intermediate, and functional method for the algorithm, only the included conversion is required. The algorithm which uses an intermediate history buffer requires exclusion changes in order to save the operation of the original and central form in their execution form, in addition to converting conversions, in their active form. Replacement status after identification Normal changes Control algorithms and application interoperability play an important role in both types of designs. In essence, it can be seen as an undo / re-change, which is done in states rather than directly operating[8].

2.1.1 Working of Operational Transformation

For example we consider a list [A; B; C] Two concurrent processes can be modified by A and B. You think that A wants to remove element C in index 2 (starting with Index index 0), which is in operation OP_A = del (2). At the same time, in the process B, add a new element to the list (i.e. 0 digit number), resulting in OP_B = INS (0; D) operation. After applying their local inventory, both procedures apply directly to their own operation (OP_A and OP_B), they receive the operations sent by other processes, without any implementation changes, process A and B (ie [D; A; B] process A And B. are found in different instructions such as in Fig. 1. for the process of D., Elements D, Elements of the Elements A process in which to move away from that a 2 to 3.

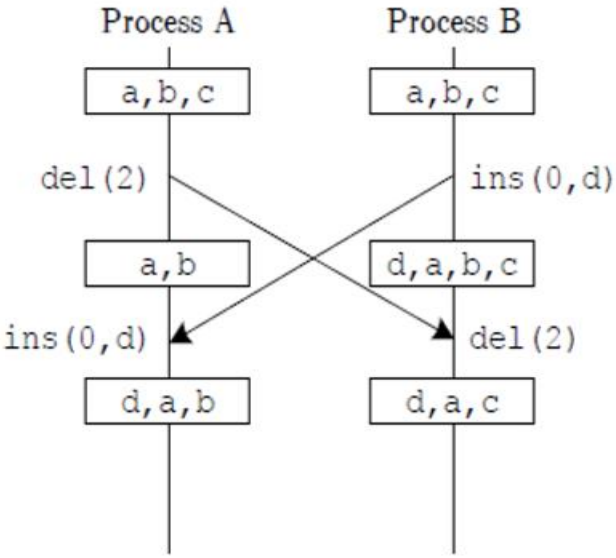

Figure 1. Without Operational Transformation[8]

Operational Transformation algorithm has improved the number of deletion operations in OP_A. Process B replaces operation OP_A replaced with Index 3, both processors appear in the same list [D; A; B] shown in Figure 2. One of the main functions of operational transformation is to maintain collaborative editing consistency. The number of compatibility models is designed for the conversion of compatible care, cooperative editing and operation. [2]

In many parts of the computing system, continuous care is a fundamental problem in things like operating systems, database systems, distributed shared memory systems, and groupware systems.

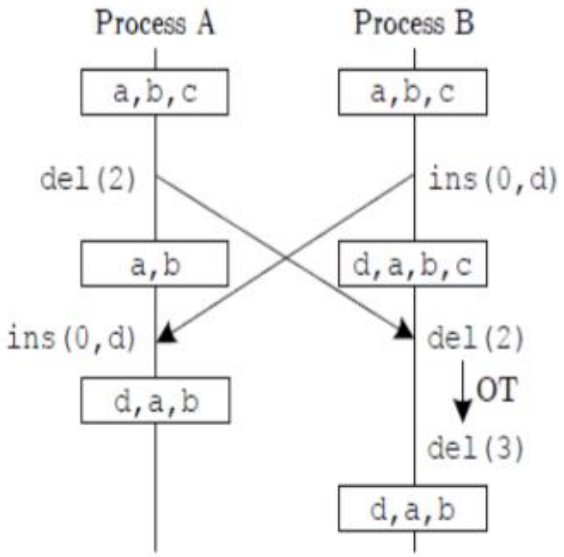

Figure 2. With Operational Transformation[8]

2.2 Diffential Syncronization

DS is a background algorithm in which there is an unmatched cycle of algebraic difference and patch operation. It is not necessary that "we can count them because the hens begin to fall" because the server-side merges into three-way trouble. Figure 2 is the ideal data flow figure for DS. Two documents (maliciously called client text and server text) are considered to be the same computer, which has no network

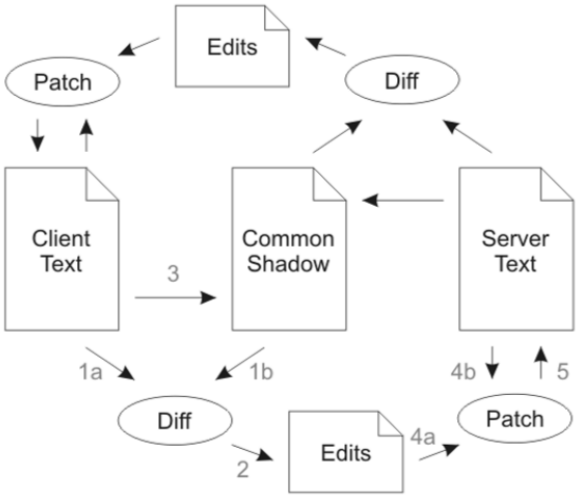

Figure 3. Differential synchronization without a network[9]

III. MOTIVATION

Development teams eventually become complex system, mainly in collaborative works environment. Relation and collaboration take place through.

Figure 4. Task Management Solution For Improved Team collaboration Source: Internet

Task management software can deliver many benefits such as:

- ✓ **Improved employee productivity:** To discuss the progress of the assigned work, employees should be able to use more time for some business meetings.[10]
- ✓ **Improved service delivery**: Get things faster than competitors.[10]
- ✓ **Lower project costs**: With everyone in loop on relevant information, there are fewer chances of errors / delays[10]
- ✓ **Supports 'work from anywhere' culture**: Most task management solutions can be accessed through a web browser and therefore can be updated remotely.[10]

IV. LITERATURE REVIEW

In this paper author describe architecture for ensuring privacy and confidentiality in incident reporting taking primarily under the consideration the large number of mobile device that can be used in creating this report and use identity clocking and message data encryption. To address this sensitive area, the confidentiality solution proposed in this paper consists of a two-step privacy protection process. Each step involves a server with a unique role in the process. The first server, used to conceal the user's identity, is the Privacy Protection Proxy Server (PPPS). The second is the Control Centre Server (CCS), used to support end-to-end encrypted

communication. Firebase Cloud Messaging (FCM) Service is used by PPPS for sending messages back to the user. The proposed architecture for a communication gateway can be very useful both to enhance user security and to support anonymous reporting of incidents, such as suspicious behaviour, criminal activity, corruption, and abuse of authority. the use of the proposed architecture in this paper It can offer the basis for citizen trust in reporting to Law Enforcement Agencies (LEAs)[11].

In this paper auhor describe While working on a forum, two users can edit a code (programming file) at the same time. Implementation includes a centralized / decentralized integration process and conversion work. Two types of changes have been proposed: Inclusion and Exclusion algorithms that use a multi-dimensional data structure to keep in its original, central, and operational form, only the included conversion is necessary only [8].

In this paper author describe DS is that it is simple and well suited for use in both novel and existing state-based applications without requiring application redesign. Client Text and Server Text may be edited at any time Scalability may become an issue as the number of clients increase. Diff and patch can be expensive operations, thus a server may become overloaded. There are two simple methods of distributing the system onto multiple servers. This would be a problem if there was very significant latency in the connection [9].

In this paper author describe the LBS server gives a private information regarding particular user location. There will be a possibility to misuse this information so using mobile crowd method hides user location from LBS server and avoid sharing of privacy information with server. In existing system user sends request to server. For that user should be connect to region of antenna. Then user send query to Server using Internet. User information store into server . Main goal of our proposed system is to hide location and private information of user. First user will connect to server and will share his all details like location information and device information with LBS server. In this proposed system are implemented to expected results . Initially all users which are going to communicate are in same region. user which is connected to LBS server and receives the query requests is User1 and next user who will request the services from Listener is User2 [12].

In this paper author describe undo approach uses selective merged to undo characters edits on documents in collaborative editing systems with operation transformation base in a group format rather than to undo them one by one. The ACE real-time collaborative editing is an open source collaborative editing system. It is written in Java and implemented in Jupiter algorithm. The work presented in this paper is focused on methods of undo in collaborative editing systems that uses centralized coordination algorithm. Our testing incorporated with the ACE collaborative editing system shows that our algorithms not only meet the correctness criteria but also supports strong efficiency and effectiveness in collaborative editing system [13].

In this paper author describe Focusing on privacy issues, but with compulsory encryption, the use of cryptographic certification schemes can guarantee of integrity. This service uses third party servers that process documents, so their content is also accessible to remote hackers, in case of direct entry qualification, ownership of government or violation of security. For the decrypted text (or encryption key) that the thief can, the provider can change the application code and send it to alternative channels (such as Web Sockets, Adobe Flash, Cookies)[3].

In this paper author describe implementation of such tool which can process files as easy as file-based encryption and has the same working speed. we use encryption of stored files. In addition, in the case of existing storage implementations, encryption must be produced entirely on the client side. When the client needs to obtain a file from cloud storage, we look for blocks that store the file in the index databases. These blocks are downloaded and decrypted, resulting file is available for the client[14].

In this paper author describe Cloud Server Authorized Cloud Support Users use outsource and shared resources in the classroom. The main problems in cloud technology are Data Conservation and Privacy Protection There are currently three parties to secure the data security of cloud resources: Users in cloud users, third party Auditor (TPA) and cloud server auditing process data grouped into owners and group users Can be done. Based on the access control policy, both data group and group users are allowed to create

and distribute data distributed in member data owners in a specific group[15].

In this paper author describe an open-ended firewall monitoring tool which can be used by cloud customers to understand the firewall's filtering behaviour. A Firewall is a component residing at the border of two networks which inspects traffic going from one to the other. All the firewalls tested work in the same way to perform basic security functions, and they all suffer from a lack of customisability and the ability to log events. The important role the firewalls play in securing these systems highlights how they have been adapted to the new environment of cloud computing [16].

In this paper author describe A comparison has been conducted for these encryption algorithms using evaluation parameters such as encryption time, decryption time and throughput. Simulation results are given to demonstrate the effectiveness of each. The present work has compared both symmetric (AES,DES,Blowfish) as well as Asymmetric(RSA) cryptographic algorithms by taking different types of files like Binary ,text and image files. we have concluded that AES is taking less time to encrypt an image files and RSA is taking less time to decrypt the image files[17].

V. RELATED WORK

A. Existing Collaborative Editing Systems Existing

The collaborative editing system can uniquely use client-server architecture. Server node Keep a constant copy of shared documents Every customer node copies the shared document. The user updates the documents shared by the local copy in the client node. All the other updates of the updates are synchronized to the server node route below , I this describe the limitations of the affiliates of four collaborative editing systems.

RCS:

This version of the RCS control system, a user can create a temporary document to clear the check. PI conflicts that occur when a user tries to change to a new version of an outdated version of the second. User Granularity of the instrument is, however, of the whole of his property by the modification of part of the species in check. RCS use locking mechanisms to detect conflicts and information. Traditionally used in the source code to manage software development, RCS has recently to withstand applications, for example, Twaki[18].

MediaWiki:

It is a great help in a group to collectively collect aggregated documents together. Users are not edited Editing different parts of the messenger More than one user should edit the same paragraph if editing the conflicts, then a user publishes himself and click to publish it. MediaWiki itself defines the changes of its own user by diff3, if it has to be changed in different parts, otherwise the affected users will be notified with the diagnostic message. MediaWiki is the largest online encyclopedia Wikipedia[18].

Google Docs:

supports the collaboration of a group of users who collaborate with collected documents together. Conflicts are edited when more than one user updates with one sentence User updates automatically synchronize to other users for a specific time interval (about ten seconds). Google Docs uses it differential-synchronization algorithm. Automatically merge changes with different users. The basic idea is similar to diff3, but if the automatic merge fails in a streaming fashion, Google Docs will notify the user via the diagnostic message[18].

Google Wave:

It means the most "liberal" editing mechanism means Google Wave users have to edit the shared document elsewhere. In all cases, you change yourself from the opposition of yourself, when users edit the overlapping area together, in other words, if more and more users delete the same data items at once, then the data items Sometimes the removal is guaranteed. For more and more users to include new data items, all the data items are protected, ensures data consistency based on Google Wave Operation Transformation (OT), blocking Google Wave for Distributed All-in-One Control Algorithm and for reasons Security properties due to both reasons, under the rational clock of Lamport's protection , which relates to his relationship before their relationship Was required to meet the person[18].

B. Commentary of Existing Collaborative Editing Systems

Atomicity of grouped operations:

There are many cases that a user wants to leave the order of Atom platform, for example cut operation after paste operation. This feature is planned to be included

in any form of block editing in the current collaborative editing system, Allows to publish their edits in batch. For example, the next release of Google Wave will increase the current keystroke by keystroke synchronization mode with block-edit mode. However, block-edit mode is not a real atom in which it buffers user edits only and sends it to other users in the batch. Due to system crashes or network interfaces, it is still possible to perform partially buffer edits on remote sites[18].

Infrastructure development:
The four described collaborative editing systems, the level of boundaries on co-operatives are very different, therefore, it is not surprising that everyone is using different enforcement techniques. For example, RCS uses the locking system, while Google Wave uses operating changes to guarantee compatibility, but it is important to remove it every time it comes out of a new type of collaboration[18].

Automatic merging in a controlled manner:
Collaborative editing systems, which fall somewhere in the collaboration-spectrum, usually merge updates automatically on best efforts. Although it can reduce manual reconciliation with users, automatic merge can produce unwanted results that can not immediately notice. The system is important to be able to limit the amount of incompatibility launched during the merger process[18].

According to the IDG study, three of the challenges slowing the adoption of collaboration solutions include security, training costs, and lack of integration with existing technologies. Box.net, a cloud-based content management provider, uniquely addresses each one of those concerns, delivering advanced security, simplicity and IT control to file sharing. Specifically:

Security:
Cloud Solution enables monitoring and management of all user activities, such as uploading and downloading files, setting permissions for individual users and for all departments, shared files password protection and time-based restrictions , File and user activity for creating and exporting and file for external users.

Simplicity:
To collaborate on the cloud, the user must create a project folder and drag and drop it from the file in the folder. To share files, send a URL or invite shareholders to view or edit if you allow anyone to edit, they can add comments to a shared folder, start discussions or Can upload files[19].

Control:
Files can be restricted to preview only, it does not download files for users but to read it; Or just upload, so they can upload files to not enter the folder. The participants, client or vendor has downloaded a file, after uploading the new content, adding a comment or informing the administrator when a new discussion is initiated[19].

VI. Security Requirement For The System And Objectives

The services also offer versioning (one is able to browse the entire history of changes suffered by the document and even roll back to an older snapshot if a mistake has been made) and read / write access controls (for individual users and/or groups). Moreover, the server authenticates each change to its respective author, so it may serve as nonrepudiation source (if trusted). One of the downsides that these services have is the use of third-party servers to process and store the documents, meaning their contents are directly accessible to whoever owns the infrastructure, their governments or, in the case of a security breach, even remote hackers [11]. Thus, we define the requirements of the solution as follows:

- Protect the user's data from potentially malicious, third party cloud server, which is the primary goal of our paper
- Use existing tools: our goal is to add privacy support to existing cloud-based document editing solutions, leveraging on their vast array of features and benefting from their market readiness
- Usability: the solution should be fast to install and easy to use, so it can enhance the users' privacy with as little as possible effort from them.
- Features: the number features that are lost when employing encryption should be kept to a minimum.

Our objective of the system is as follows.

- ✓ Improving the confidentiality and privacy of the user data from the service provider.
- ✓ Prevent the unauthorized access to cloud computing infrastructure resources.
- ✓ Prevent the information leakage from the service provider.

VII. SECURITY THREATS

In this section, we identify ten types of threats collaborative security aims to prevent. These threats are collected basically from two sources:
1) The surveyed literatures in which certain threats are prevented by collaborative security systems;
2) The typical security threats Some collaborative security systems aim to address the issues of general threats, such as intrusion and malware. We hence conclude the typical and concrete threats in terms of these common taxonomies of threats. For example, malware may cause the privacy leakage, or privilege escalation in an attack. Then, systems which can prevent malware can naturally resist the attacks of privacy leakage and privilege escalation. More details about the correlation [20]

Privacy Leakage:
A potential risk of downloading online software is the possibility of exposing users' sensitive data such as account credentials, preferences, contacts, etc. Attackers may use some techniques like brute force attacks, man-in-the-middle attacks, and phishing tactics in order to steal sensitive data. Privacy leakage through downloading malicious software has been exacerbated in recent years on mobile devices with the rise in popularity of mobile applications[20].

Privilege Escalation:
It is common to grant privileges to an application upon installment, however vulnerabilities in these applications can result in an increase of privilege authorizations, data tampering or the disclosure of information. Permissions on Android, for example, must be explicitly identified and applications cannot access the device's resources until the installer grants it the required permissions. However, many malicious applications circumvent the permission mechanism and exploit indirect tactics to access sensitive resources[20].

Authentication Violation:
Authentication is a security scheme used to identify whether a user is as it claimed, using signature and encryption technologies. However, some malware may impersonate as other applications in order to carry out these particular behaviors[20].

Spam:
While it is sometimes treated more of an annoyance than a threat, by sending myriad messages (e.g., emails), attackers can post an advertisement or spread viruses through spam. From another prospective, they can result in high overhead of traffic which can cause denial of service[20].

Denial of Service:
In a denial of service attack, an attacker tries to make a host, or services on this host, unavailable to its intended users. Availability may be the most concerned property in networks. An attacker may crash services on a host, e.g., employing a vulnerability existing in a service to disturb its normal operation, and thereby avoiding any other user of using that service; it can also flood a host by launching a huge amount of requests to prevent other users from connecting to the host[20].

Malicious Code:
Execution In this attack, malicious code is deployed somewhere in advance, and attackers can exploit existing vulnerabilities of systems to execute the malicious code[20].

Abuse of Functionality:
To launch an attack, attackers may manipulate one or more functionalities of systems, which should not be used arbitrarily. By breaking this security policy, the attackers can alter or influence the normal behaviors of the system, or destroy the integrity of information [20].

VIII. CONCLUSION AND FUTURE SCOPE

In this paper, Security of Collaboration systems needs to be secure at some extent so no one other than authorized user can access it. Compared to traditional individual security, the intention of collaborative security is to share dependable information to provide better security for large systems. several challenges with the current structure of collaborative security systems will be proven to limit the extent of the effectiveness of this type of system.

IX. REFERENCES

[1]. Rasha Fouad AlCattan, "Integration of Cloud Computing and Web2.0 Collaboration Technologies in E-Learning,". International Journal of Computer Trends and Technology (IJCTT) – volume 12 number 1 – Jun 2014

[2]. Wenbing Zhao, Mamdouh Babi, William Yang, Xiong Luo, Yueqin Zhu, Jack Yang, Chaomin Luok, Mary Yang, "Byzantine Fault Tolerance for Collaborative Editing with Commutative Operations", 2016 IEEE.

[3]. Florin Stancu, Mihai Chiroiu, Razvan Rughinis, "SecCollab-Improving Confidentiality for Existing Cloud-based Collaborative Editors," 2017 21st International Conference on Control Systems and Computer Science.

[4]. Huanhuan Xia, Tun Lu, Bin Shao, Xianghua Ding and Ning Gu, "Hermes: On Collaboration across Heterogeneous Collaborative Editing Services in the Cloud," Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design.

[5]. Sheng-Cheng Yeh,Ming-Yang Su,Hui-Hui Chen,Chun-Yuen Lin, "An efficient and secure approachfor cloud collaborative editing," Journel of network and computer application 36(2013).

[6]. "Google Docs https://docs.google.com/.MumtazAhmad" Collaborative Distributed Editing "IEEE 2015.

[7]. Mandeep Kaur, Manpreet Singh, Harneet Kaur, Simran Kaur "Operational Transformation In Co-Operative Editing" international journal of scientific & technology research volume 5, issue 01, january 2016.

[8]. Neil Fraser ,"Differential Synchronization". in Proceedings of the 9th ACM symposium on Document engineering. ACM, 2009,pp. 13–20.

[9]. http://www.smallbiztechnology.com/archive/2013/09/5-task-management-solutions-for-improved-team-collaboration.html

[10]. Christos Chatzigeorgiou, Lazaros Toumanidis, Dimitris Kogias, Charalampos Patrikakis,Eric Jacksch "A Communication Gateway Architecture for Ensuring Privacy and Confidentiality in Incident Reporting" IEEE 2017

[11]. Sarika Patil, Sonali Ramayane, Megha Jadhav, Prof.Pravin Pachorkar "Hiding User Privacy in Location Base Services through Mobile Collaboration: A Review" 2015 International Conference on Computational Intelligence and Communication Networks

[12]. Mamdouh Babi,Wenbing Zhao "Selective Merged Undo for Real-Time Collaborative Editing" 2016 IEEE.

[13]. Artem A. Maksutov, Stanislav V. Kutepov, Alexander S. Hrapov" Efficient Processing and Storage of Data on Untrusted Cloud Storage Services" 2017 IEEE

[14]. Anjali R. S., Aswathy Ravikumar" Preserving Privacy in Public Auditing for Shared Cloud Data"IEEE 2016

[15]. Yan Huang and David Evans, "The Role and Security of Firewalls in IaaS Cloud Computing" 2015 10th International Conference on Availability, Reliability and Security.

[16]. Madhumita Panda,"Performance Analysis of Encryption Algorithms for Security" International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016

[17]. Qinyi Wu ,Calton Pu "Modeling and Implementing Collaborative Editing Systems with Transactional Techniques"IEEE 2010

[18]. The Cloud: Reinventing enterprise collaboration

[19]. Guozhu Meng, Yang Liu, Jie Zhang, Alexander Pokluda, Raouf Boutaba," Collaborative Security: A Survey and Taxonomy".