|| Volume 6 || Issue 3 || March 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

A SCALABLE AND SECURE COLLABORATIVE TRUST ASSESSMENT TECHNIQUE OVER INTER-CLOUD STRUCTURES

Abdul Mateen[1], Mohammed Abdul Rawoof[2], and Mohammed Sanaullah Qaseem[3]

Research Scholar, Dept. of Computer Science & Engineering, NSAKCET, HYD [1]

Associate professor, Dept. of Computer Science & Engineering, NSAKCET, HYD [2]

Professor, HOD, Dept. of Computer Science & Engineering, NSAKCET, HYD [3]

---------- ***----------

Abstract: - In recent days, social networks are being used as a medium of communication and for sharing data and information with others. The privacy of users may be compromised on such social platforms. Sharing of jointly owned information also poses a privacy threat. For example, when one of the users tries to shares data that is associated with multiple other users, the privacy of a few users might be at risk as diverse users, in general, have diverse views about how the data in the system could be accessed and who should be permitted to access the data. Hence we require a sharable data management technique to handle the above-mentioned confidentiality concerns. The development of such a technique is of immense use in the collaborative environment. We put forward a novel technique that is based on trust to achieve mutual privacy. The core principle of this technique is that a user can decide whether a data file or item could be posted or uploaded based on the collective view of all the associated users. The trust value inputs given by the users are used to calculate the weighted average of the user's views and the values are revised as per the user's opinion about confidentiality. Also, the users can strike a balance between preserving the confidentiality of the data item and data sharing by adjusting the above-mentioned parameter – Trust based weighted average. Replication of the proposed technique has proved that it promotes the users to consider the confidentiality aspect of the information and the proposed approach fetches greater profits.

Keywords: - *Intercloud, trust evaluation, privacy, reputation, cloud computing.*

----------***----------

I.INTRODUCTION

In recent times, social networks such as Twitter, Facebook, Google, etc, are playing an important role in social communication s. They have become an integral part of the process of making social connections. Millions of people around the world post data in various forms and formats like text, videos, posts, messages, photos, etc on social networks on the internet. Such information frequently has private data of the users. If such private information that is posted on these social networking sites could be accessed by unauthorized people, the privacy of the data owner who posted the information would be compromised. Such confidentiality concerns have always been a prime element in studies associated with social networking sites. The social networking sites would have to first control or avoid data access violations to protect the user's confidentiality and integrity. The users can also set some settings at their end about who can access their information. An access regulation methodology specifies which users can access the data owner's information. The existing social networking sites make use of the user relationship to differentiate between the approved and unapproved users. For instance, a Facebook user can mention if their data or posts could be viewed by their friends, particular groups, or everyone. All the existing privacy regulation techniques that are employed in the existing social networking sites have constraints on the users who would like to access the data. We do not observe any kind of restrictions or constraints on the users who post or upload the information. As a result of this one-sided access regulation, the users who post the information might breach the privacy of other users. Below mentioned is one such scenario: Let us assume that user X posts a photograph of user Y and himself and shares it with his colleagues. If user Y regards that photograph as private information and he is not acquainted with colleagues of user X, then the privacy of user Y would be breached. In the above-mentioned scenario, the photograph is owned by both user X and user Y. Therefore the privacy guidelines mentioned by user X must be consistent with the privacy guidelines of user Y. If that is not the case, then user Y would have his privacy

violated. It is very natural to have a data item owned by multiple individuals on social networking sites. All the owners of the co-owned data should come together to manage the confidentiality of the data item. In recent times, multiple studies are happening in this area to resolve the problem. Most of the existing studies try to address the issue by identifying the conflicts between the confidentiality guidelines of the various users corresponding to a particular data item and then create a cumulative policy that can address the differences to the maximum possible level. The confidentiality regulation mechanism in the existing system is governed by the group of users with whom the data has been shared. In general, there is a negotiator who does the job of collecting the confidential guidelines off multiple users and comes up with a cumulative policy by using a certain aggregation mechanism. However, the privacy loss is not entirely removed as there would be still some conflicts existing and the aggregated policy has still not provided a complete resolution for the problem of collaborated confidentiality management. The important aspect that must be addressed in this scenario is that how can we strike a balance between data sharing and safeguarding the privacy of the users. Unlike the existing system where a negotiator collects the privacy requirements and comes up with an aggregated regulatory mechanism, we design a novel approach where the user who would like to post the data would consider the confidentiality concerns of all the owners who co-own the data item and comes up with A mutual decision that is agreed by all the owners. Some of the previous studies on this topic generally consider and make use of the tagging mechanism to identify the Co-owners. In this case, the negotiator would be able to identify all the involved users and can come up with an aggregated confidentiality guideline. However, it is not always necessary that all the users who post the data items should necessarily tag all the involved users. This makes the existing mechanism difficult and causes confidentiality loss for the users who are not identified. Taking this scenario into account, we recommend a technique in which the user who is posting the data must consider the opinions of all involved users before posting the data. A novel aggregated scheme is built which is based on voting and weighing the trust parameter of the opinions of various involved users. When the user wants to post a data item, he will define the confidentiality regulation and inform the involved users to approve or disapprove of the defined regulation. The significance of the approval is dependant on this trust parameter value that exists between the users. The votes or approvals are aggregated and the data item is allowed to be posted only when the cumulative approval satisfies a particular condition. It has to be noted that the trust value parameter is not fixed between the users. A user can lose confidence or trust if he does not cater to the privacy needs of the other individuals on the system. If the data item posted by the user causes privacy lost to another user, then his trust parameter value decreases. Also, the trust parameter value increases when he accommodates other's views. The relationship between confidentiality loss and trust parameter value indicates that The user should always take into consideration the opinion of all the involved users instead of taking an individual decision while posting co-owned data.In the recommended solution of collective privacy management by using trust parameter, we also introduce a threshold parameter using which the user decides of posting the data. To elaborate this, a higher threshold value specifies that the user generally does not prefer sharing data with others, and only when most of the involved users with high trust values have agreed to post the data item, only then the item can be posted. It is by adjusting this threshold parameter, one can strike a balance between safeguarding the privacy of users and data sharing. When the user frequently posts data items on social networking sites it is difficult to define the threshold value and it is incorrect to use a fixed threshold value. Hence we define the selection of threshold value as a serial decision-making problem and apply higher confidence bound guidelines to solve the problem of defining the threshold value in real-time environments.We prove that the recommended methodology is far more efficient when compared to the existing mechanisms to safeguard the privacy of users. A balance can be achieved between data sharing and privacy preservation by using the threshold value.

II LITERATURE SURVEY

"Privacy and security for online social networks: challenges and opportunities"

Social networking platforms are nowadays working as an excellent medium of communication and social interactions. These systems have a huge amount of private data collected from billions of users. The purpose of social networks is to collaborate and share information with the intended audience. However, some privacy and security issues arise when unintended users try to access the information. Exposing personal identity and other relevant information on social networking sites might lead to many security issues like spamming, phishing, reputation. We also have opportunities to address the above-mentioned issues and make the social networking sites and platforms a safe place to share data. The design and security challenges concerning the architecture of social networking sites have been discussed in this paper and some techniques that are under development to mitigate these issues are highlighted.

"Information security and big data: privacy and data mining"

With the exponential growth of the Internet, E-Commerce, social networking platforms, and data mining security threats and leaking of confidential information are posing great risks

for cybersecurity. One of the latest and emerging topics for research is the privacy-preserving data mining technique where the objective of the data mining Easter understand and explore the underlying patterns in the data and at the same time keep the customer information safe and secure. Data mining is a process that involves various activities like data collection, data cleaning, data transformation, and data loading. The private information of the individuals might be exposed in these stages. Hence in this paper, we introduce the people associated with this processes namely data provider, data collector, data miner, and decision-maker, and try to come up with ways to resolve the privacy issues that arise in each stage of data mining and help to protect the sensitive information off the user.

"A framework for categorizing and applying privacy preservation techniques in big data mining. "

In this paper, some practical approaches of how to preserve the privacy of the user in big data mining are discussed. some of the techniques discussed are:

i. anonymization- at a technique where the personal identity information is removed and content is generalized

ii. reconstruction and modification- helps protection of sensitive information from unnecessary detection by mining algorithms

iii. provenance Methodologies

iv. restriction methodologies

v. agreement and trade methodologies etc

III SYSTEM ANALYSIS

Existing System:

In the existing systems, the approach to resolve the conflicts that arise during data sharing is to find the reasons for the conflicts and try to resolve them to the maximum extent possible. These approaches do not enforce any guidelines for sharing data that involves multiple users. Aggregation of privacy policies, space segmentation approach, negotiating party which tries to aggregate and resolves the conflicts call some of the approaches used to reduce the privacy loss in the existing social networking sites. However, none of the approaches seems to resolve the problem completely. the role of trust in handling the privacy loss issues is very important to solve this problem. Trust-based mechanisms have not yet fully evolved in the existing environments.

Disadvantages:

1. policies to control the access are not defined.
2. Collaborative confidentiality management is not in place
3. Users can go ahead and share data without seeking the permissions of all the involved users
4. privacy lost cannot be controlled before sharing of data

5. Proposed System:

In the recommended system, we define a threshold value to decide whether the data item or post can be shared or not. The higher the threshold value the lesser is the scope for sharing the data. However, it is important to strike a balance between data sharing and safeguarding the privacy of other involved users. And it is also quite common to keep sharing data on social networking sites. Hence it is important not to restrict data sharing and at the same time, we need to be considerate about the privacy needs of other people on the platform. Hence the threshold value cannot be a fixed value and it needs to be dynamic. Thus we apply upper confidence bound policy using the bandit approach and voting mechanism to dynamically calculate the threshold value and make a decision if the data item can be posted.

Advantages

1. Policies to control the access can be defined by each user
2. Collaborative confidentiality management can be enforced using the above process.
3. users need to seek permission before posting the content from all the involved users.
4. Privacy loss can be controlled well ahead before sharing the data as the user gets to know whether the sharing of data results in privacy loss or not.
5. Defining the threshold value and voting comparing it with the words received will help to decide whether the data item can be posted or not.

IV IMPLEMENTATION

There are two modules in this project. They are:

1. Admin
2. User

Admin Module:

In this module, the admin has to first login with his credentials. On successful login the admin can perform various activities like viewing and authorizing user requests, view access control policies, view the Trust values of users, view the shared data items, view the posts with opinions and votes, view the vote chart, etc.

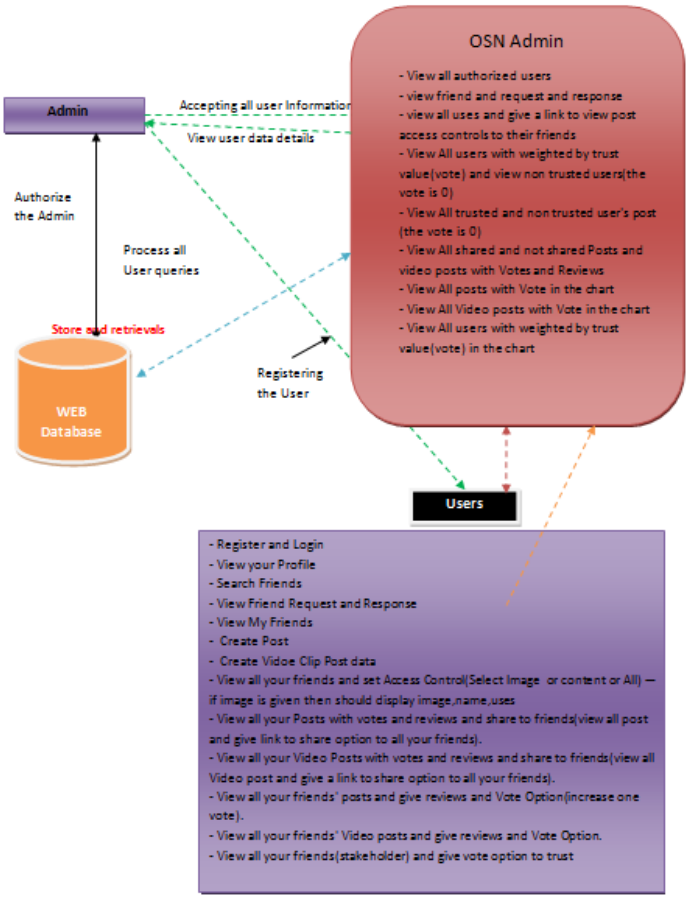
User Module:

In this module, the user has to 1st register on the system by giving the details like username, gender, profile picture, date of birth, etc. The login request would be sent to the admin for approval. Once the admin approves the login request, the user would be able to log in and post data and perform other activities such as view profile, search for friends, view friend request, create posts view friend requests view posts with votes and reviews, view friend posts and give reviews, etc

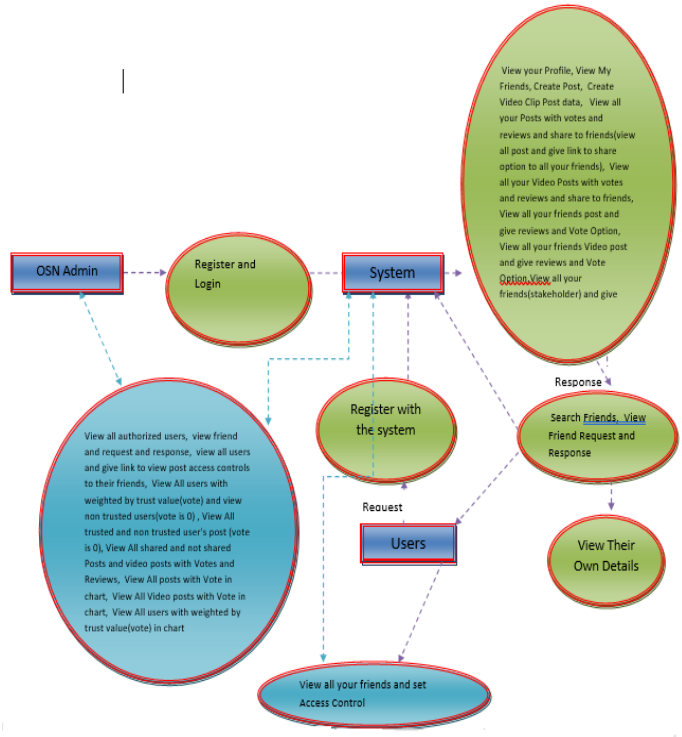
|| Volume 6 || Issue 3 || March 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

V SYSTEM DESIGN

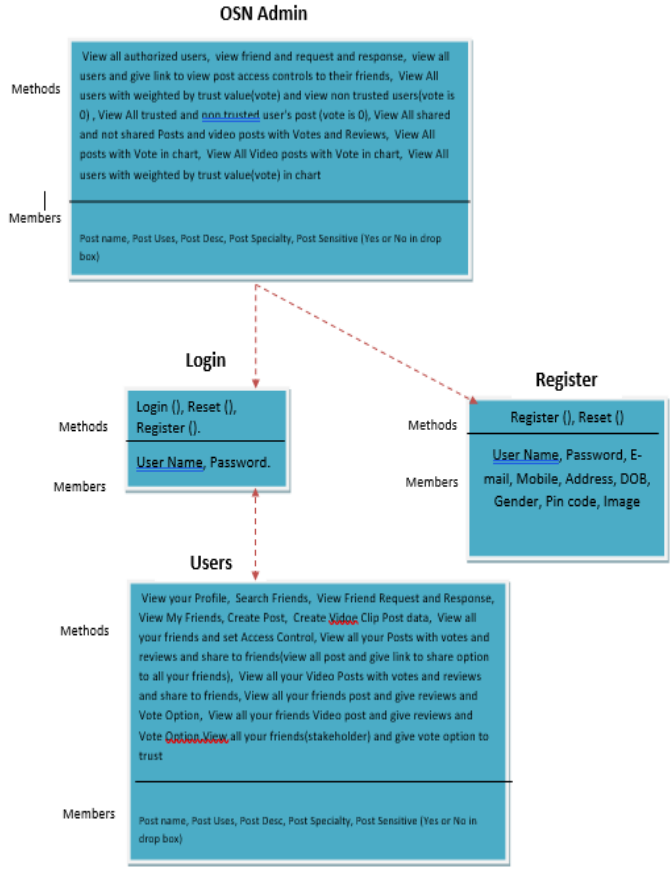
Architecture Diagram:



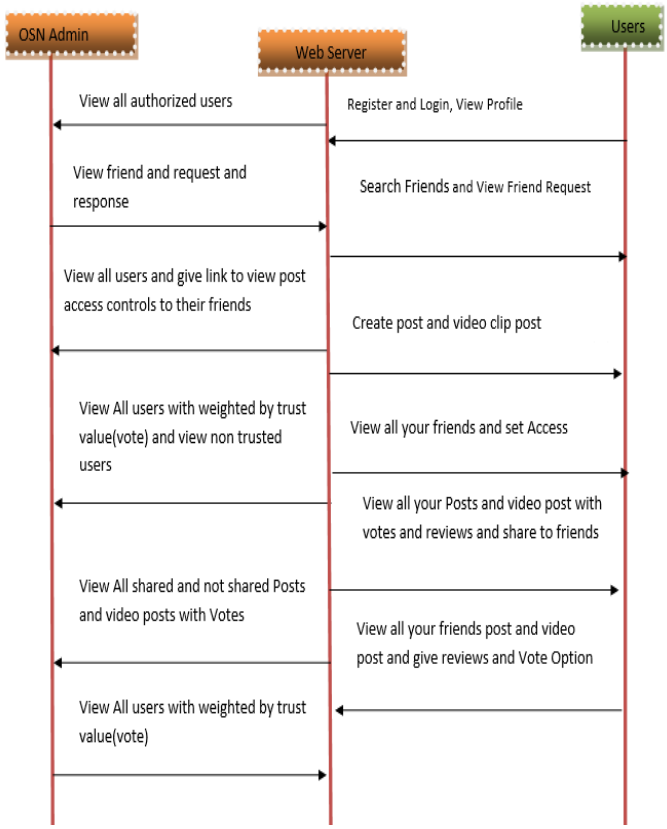
Data Flow Diagram:



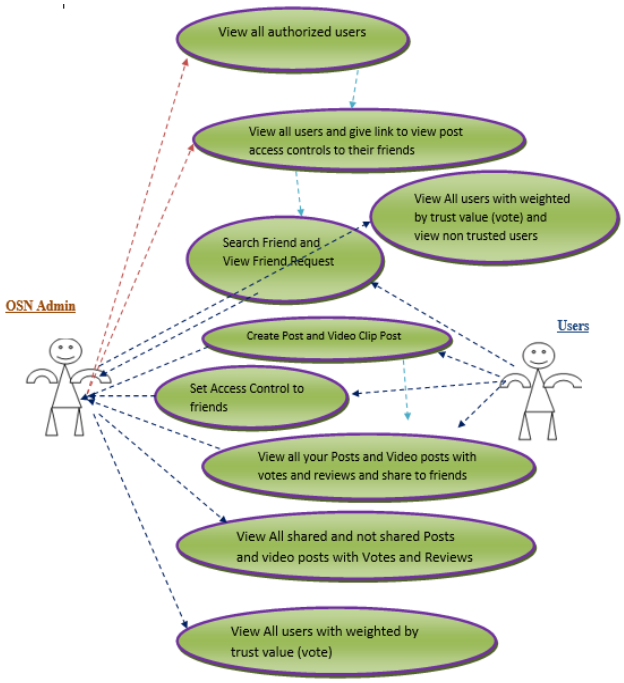
Class Diagram :



Sequence Diagram :



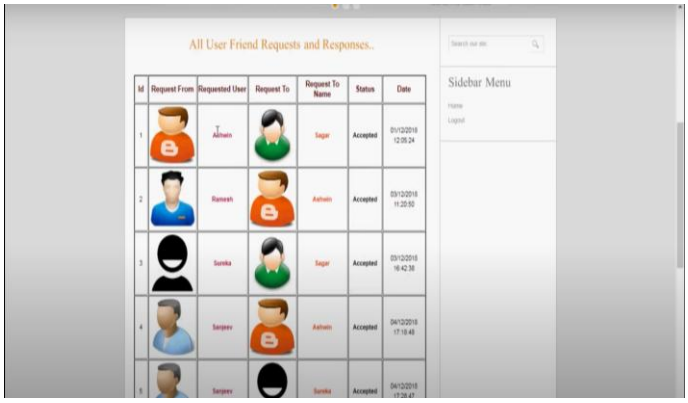
Use Case Diagram:



VI PROJECT EXECUTION AND TESTING

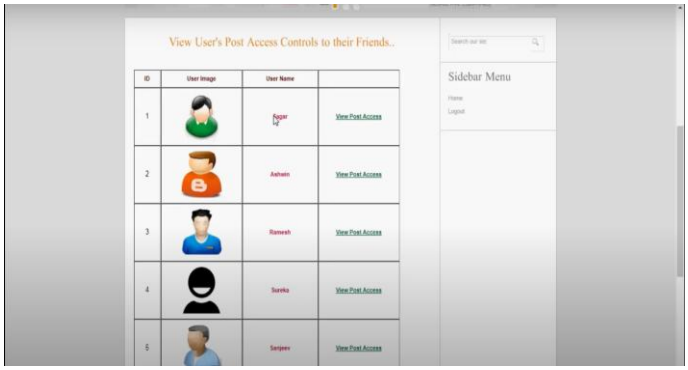
View Friend requests and responses:

On this page, the admin can view the status of friend requests between various users.



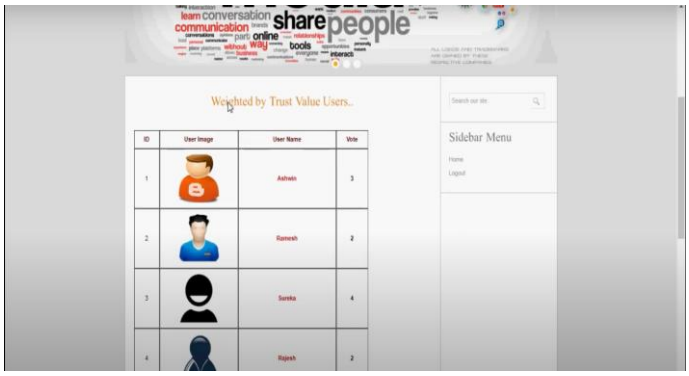
View User's Post access control to their friends:

On this page, the admin can view the post access control given by one user to another user. The second user will be able to review only based upon the access policy set by the first user.



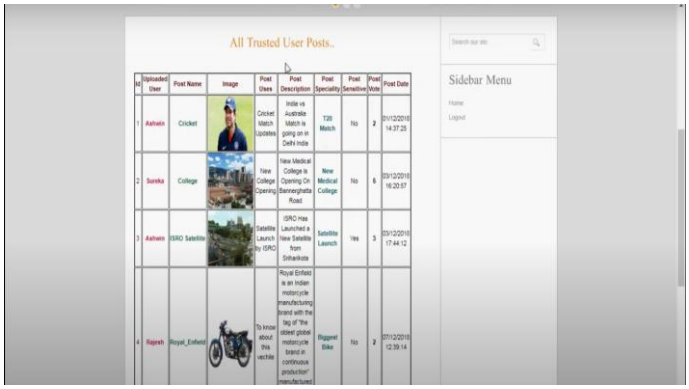
View the users weighted by Trust:

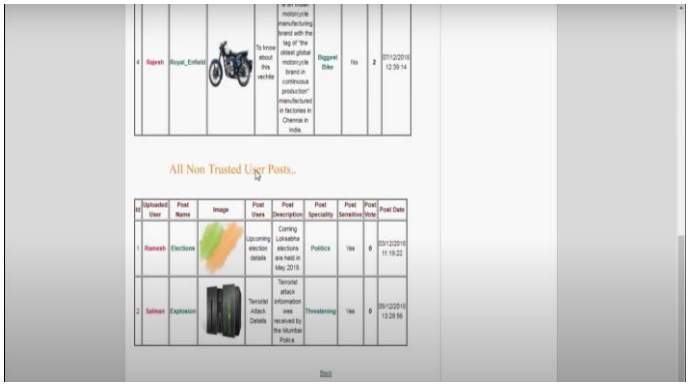
On this page, the admin can view the votes given to various users based on the trust values. The higher the votes, the higher is the trust value.



View all Trusted user posts:

On this page, the admin can view all the posts posted by the trusted And untrusted users.



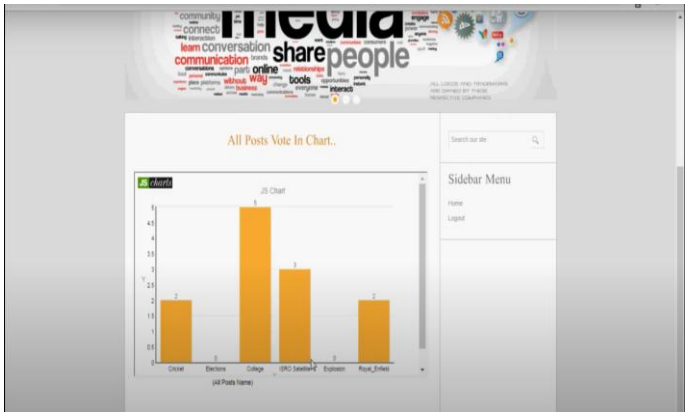


View user reviews on posts:

On this page, the admin can view the review comments given by the users on their friend's posts

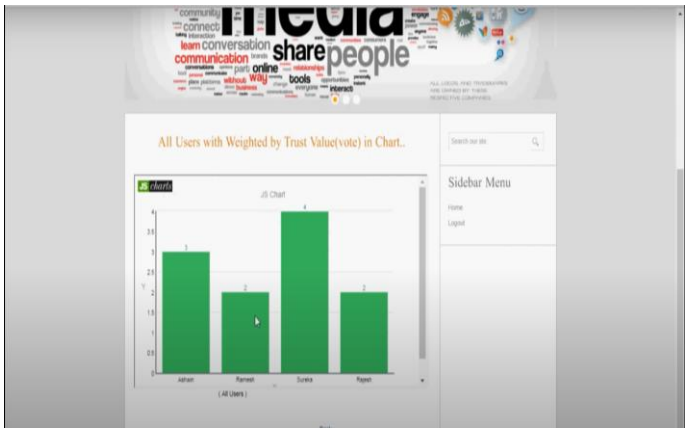
View all posts in the Vote chart:

The friends can review and vote for the posts. All the votes for a particular post are aggregated and displayed on the vote chart.



View all users with weighted by Trust value in the chart:

Every user can assign a trust value to their friend. All the trust values assigned in this way are aggregated and displayed in the vote chart below



User Login:

Using this page the users' can log in to the system to share data and content with their friends.

User registration:

using this page the user has to 1st register on the system by giving details like name, password, date of birth, profile picture, etc

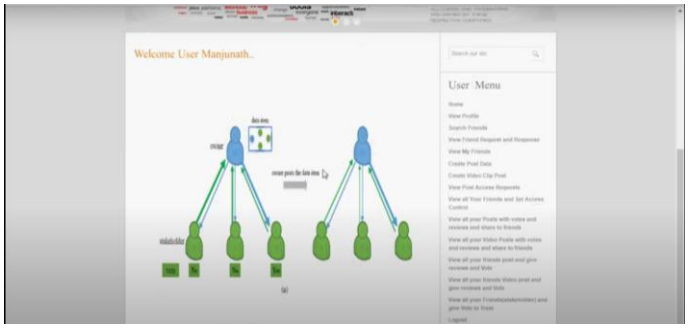
User waiting for Admin Approval:

This screen is displayed when the user registers on the system and waits for admin approval.

User Home:

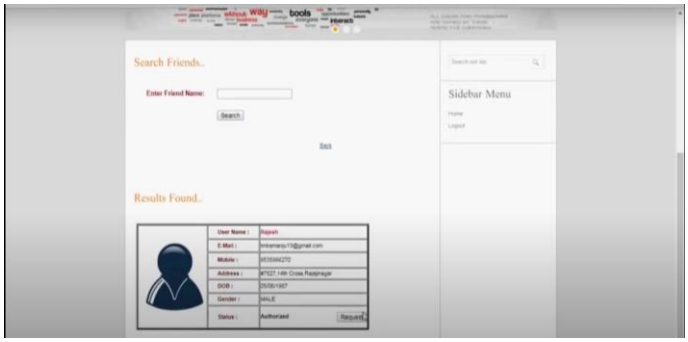
Once the admin approves the user registration, the user can log in from the login page and get redirected to the homepage. On this page he can perform various activities Lake creating posts, searching for friends, reviewing and voting for friends posts,

doing the trusted and untrusted posts, set trust values and access policies for friends, etc



Search Friends:

this page is used by the user to search for friends and send a friend request.



View Friend Requests:

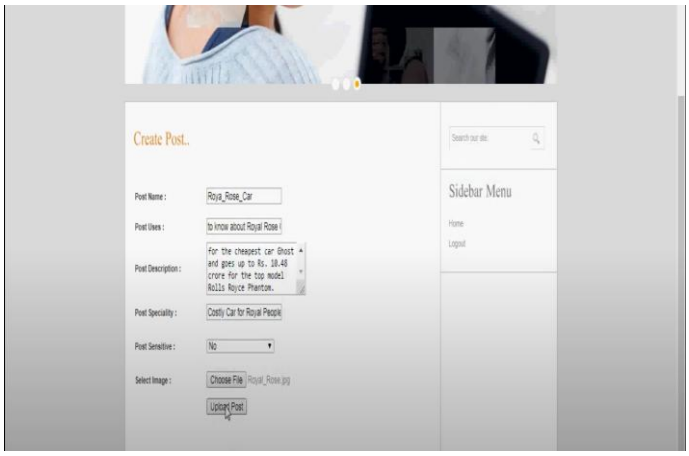
On this page, the user can view the friend request he received and approve them

View All Trusted and Non-Trusted Users:

On this page, the user can see a list of all the trusted and non-trusted users.

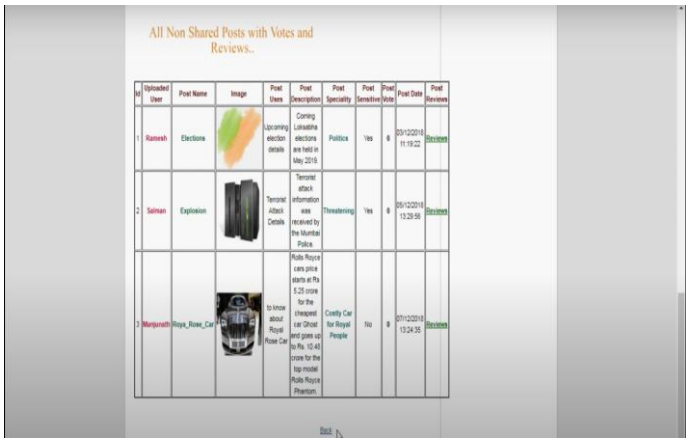
Create Post:

Using this page the user can create posts and publish them on the social networking site.



View all shared posts with votes and reviews:

On this page, the user can view all the shared post and their reviews.

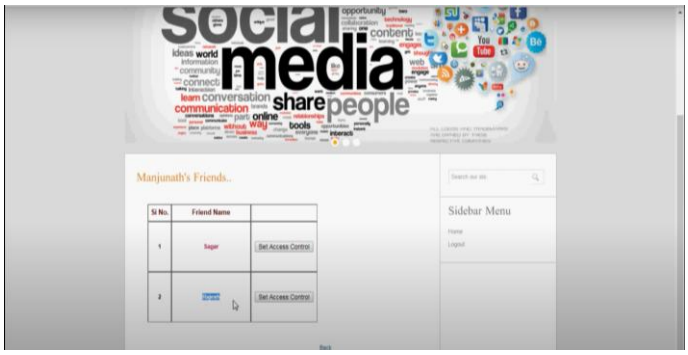


Share posts to Friends:

Using this page the user can share his post with his friends

Set Access control for Friends:

Using this page the user can set access control for his friends like if their friends can access images or content or everything.

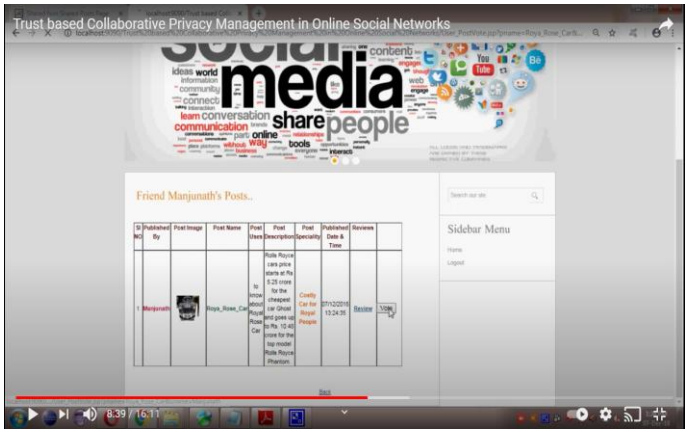


Give reviews for Friend's posts:

On this page, the users can review their friend's posts and submit them.

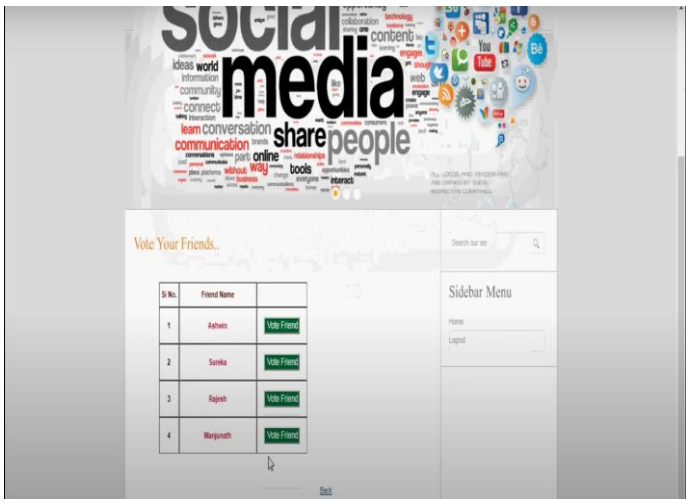
Vote for Friend's post:

On this page, the users can vote for their friend's posts. All the votes further posts are aggregated and displayed in the vote chart



View Friends and give the vote to Trust:

On this page, the user can view the friends and sign a trust value to his friend. If the friend takes into consideration his privacy, he will be given a higher trust value otherwise the trust value could be decreased.



View Friend's posts:

On this page, one can see the friend's post only if the friend has set up the access control policy for this user. A link to request access has been given.

VII CONCLUSION

The confidentiality concerns that arise due to the sharing of mutually-owned data on the social networking platforms are studied in this paper. We recommend a trust-based privacy management technique to overcome the privacy loss that happens when the data corresponding to multiple owners is shared. This mechanism helps all the involved users to collaborate and come up with a cumulative view. This cumulated opinion is compared with an existing threshold value and the final decision of posting the data item is taken based on the result of the comparison. If a user has more trust in a stakeholder, more value is given to the stakeholder's opinion. The trust value of a user is dynamic and changes with every data posting activity. If a user does not take into consideration the opinion of another user while sharing data, the trust value of the user decreases. Hence, we define a threshold to take the final call is the data item should be posted or not. Experiments have been conducted using real-time data and test data to validate the technique. The results Indicate that whenever he posts data without getting the required permissions That is the loss of privacy compared to the posting of data when the user's opinion is collected. It has also been noted that dynamically calculating the threshold value using UCB policy has fetched greater profits when compared to her fixed threshold value.

Future Enhancement:

In future we would like to extend this project to have a dynamic threshold value for each user-friend combination and maintain this in a database.

REFERENCES

[1] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," IEEE Network, vol. 24, no. 4, pp. 13–18, July 2010.

[2] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," IEEE Access, vol. 2, pp. 1149–1176, 2014.

[3] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, "A framework for categorizing and applying privacy-preservation techniques in big data mining," Computer, vol. 49, no. 2, pp. 54–62, Feb 2016.

[4] M. Qiu, K. Gai, and Z. Xiong, "Privacy-preserving wireless communications using bipartite matching in social big data," Future Generation Computer Systems, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17301449

[5] C. Fiesler, M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. Hutto, S. Morrison, P. Khanipour Roshan, U. Pavalanathan, A. S. Bruckman, M. De Choudhury, and E. Gilbert, "What (or who) is public?: Privacy settings and social media content sharing," in Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, March 2017, pp. 567–580.

[6] A. C. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in Proceedings of the 18th ACM International Conference on World Wide Web, April 2009, pp. 521–530.

[7] H. Hu, G.-J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," in Proceedings of the 27th ACM Annual Computer Security Applications Conference, December 2011, pp. 103–112.

[8] J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Transactions on Knowledge and Data Engineering, vol. 28, no. 7, pp. 1851–1863, July 2016.

[9] P. Auer, N. Cesa-Bianchi, and P. Fischer, "Finite-time analysis of the multiarmed bandit problem," Machine learning, vol. 47, no. 2-3, pp. 235–256, 2002.

[10] H. Hu, G.-J. Ahn, Z. Zhao, and D. Yang, "Game-theoretic analysis of multiparty access control in online social networks," in Proceedings of the 19th ACM Symposium on Access Control Models and Technologies, New York, NY, June 2014, pp. 93–102.