International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 3 ǁ 2021 ǁ PP. 55-62

Privacy Preserving and Data Integrity in Social Networking

Narendra Manikrao Jathe
Department of Computer Science, Shrimati Narsamma Arts, Commerce and Science College, Amravati, India

Abstract
Today's social networking services require users to trust the service provider with the confidentiality and integrity of their data. But with their history of data leaks and privacy controversies, these services are not always deserving of this trust. Indeed, a malicious provider could not only violate users' privacy, it could equivocate and show different users divergent views of the system's state.
Such misbehavior can lead to numerous harms including surreptitious censorship. In light of these threats, this paper presents data security framework for social networking applications that can be realized with an untrusted users. Prior secure social networking systems have either been decentralized, sacrificing the availability and convenience of a centralized provider, or have focused almost entirely on users' privacy while ignoring the threat of equivocation.
On the other hand, existing systems that are robust to equivocation do not scale to the needs social networking applications in which users may have hundreds of friends, and in which users are mainly interested the latest updates, not in the thousands that may have come before. To address these challenges, we present a novel method for detecting provider equivocation in which clients collaborate to verify correctness. In addition, we introduce an access control mechanism that offers efficient revocation and scales logarithmically with the number of friends. We present a prototype implementation demonstrating that privacy preserving and data security provides latency and throughput that meet the needs of a realistic workload.
Keywords: *Social Networking Sites (SNS), Information Assurance (IA), OSN*

Date of Submission: 23-02-2021 Date of acceptance: 07-03-2021

I. INTRODUCTION

The phenomenon of social networking sites (SNS) introduced to the public about five to six years ago have changed the way people communicate with each other on the Internet. Some social networking sites like Facebook attracted millions of users in the first years of their operation and their operators claim to have hundreds of millions of users worldwide. The main benefit of the majority of social networks is to facilitate new friendships, online interaction and communication for which the user profile is the crucial component for establishing connections. In the profile a user can share information such as his name, photos, address, interests, political views, etc. Several studies showed that the members of social networks not only disclose true information about themselves, but provide even more information than they would do in real life [1, 2]. With the development of information retrieval and search engine techniques, it becomes very convenient to extract users' personal information that is readily available in various social networks. Malicious or curious users take advantage of these techniques to collect others' private information. Therefore, it is critical to enable users to control their information disclosure and effectively maintain security over online social networks. So, privacy, and other ethical and statutory obligations, generally imposes collections of system goals, each of which is managed in its own right. For example, a business goal of 'comply with data protection and human rights legislation' is interpreted as a list of security goals that are contained within statutes and related documentation (advice, orders), or established as best practice.

These include protection goals (e.g. confidentiality and integrity of personal data) as well as functional requirements (e.g. users must be able to access and correct records held about themselves, data must be deleted after use).As a consequence there is no distinctive goal of 'privacy' that requires special treatment; each of these obligations are treated as a separate system goals. Security is difficult to measure because so many security attributes are not mutually commensurable. Perhaps for this reason, network security is often measured in terms of Information Assurance (IA).

1.1 Social Network Providers and Their Customers

Social network providers offer social networking services to the users and may further provide additional interfaces and services to other customers. These customers may come from different domains and pursue various goals.

In particular, sponsors belong to customers who advertise their services to the users through the OSN

platform. Their advertisements may be of different kinds: plain commercial sponsors buy banner space or other marketing services from the SNP to advertise their products; SNS frequently contain "market pages" at which users can publish classified ads, job offers, and the likes, for which they may be billed. Also sponsors may create commercial interest groups or profiles inside the OSN.

Another type of OSN customers are third party service providers, who extend the content and functionality of SNS with their own applications. These applications such as quizzes and games are typically executed on the servers under control of these third parties connected to the SNS via appropriate APIs.

Often these applications have extensive access to the personal data of OSN users. Finally, all sorts of data analysts may act as customers of SNP. These customers typically have data mining interests and may also get access to the personal information of users and their activities within the OSN. The analysis carried out by data analysts may serve different purposes, including scientific research (such as statistics, social behavior, or network-relevant aspects) and non-scientific data mining, typically for commercial purpose such as marketing.

1.2 Privacy in Social Networks

Next, we survey user privacy expectations for social networking sites. The goal of our design is to provide a platform that satisfies these expectations by guaranteeing that a user's data is only accessible to another user through the programming platform if it can be viewed by that same user through the standard web interface.

1.3 User Expectations

Past work demonstrates that users have strong expectations for privacy on social networking sites. A social phishing attack experiment [10] harvested personal data from a social networking site by screen scraping and used it to construct phishing e-mails. Users expressed anger that their information could be collected and used in such a manner without consequences, with users protesting that their profile data should be protected [10]. Additionally, when Facebook launched the Facebook Beacon, which correlated activities on other websites with Facebook profiles, user outrage forced Facebook to retract the program [14]. These strong reactions illustrate that users believe social networking sites have a responsibility to shield their data.

Privacy expectations in social networks are based on relationships. Typical social networks support friends and networks with privileged access.

Friends: Friendships are a defining characteristic of social networking sites, and friends receive access to personal data. Friendships require acceptance by both parties. Some sites may extend privileges to the second or third degrees of connection.

Networks: Social networks also support networks, where members have some access to each other. Bebo and Facebook associate access controls with school attendance. Alternately, self-defined regions can be considered a network, and privacy controls may be associated with the chosen location (e.g., Friendster users can limit their profile visibility to certain continents).

Public visibility: Sites define some subset of a profile (such as the user's name and affiliation) visible by default for searching and identification. Most sites also allow users to relax or strengthen their definition of public information.

II. LITERATURE REVIEW

Ariel J. Feldman et. al. [1] provide a general framework for social networking applications built around an untrusted service provider. The system had to both preserve data confidentiality and integrity, yet also remain e scalable, and usable. Towards these goals, we present a novel method for detecting server equivocation in which users collaborate to verify object histories, and more efficient mechanisms for ensuring fork consistency based on history trees. Furthermore, we provide a novel mechanism for efficient access control by combining persistent authenticated dictionaries and key graphs.

Chi Zhang et. al. [2] discussed the security and privacy design issues on online social networks and pointed out a few research directions for mitigating the design conflicts between the various design goals of OSNs. However, an ultimate solution will require experts from the social science and network security communities, industry, regulatory bodies, and all other relevant communities to collaboratively make decisions on both secure mechanisms and policies. This article is intended to provide a starting point for developing effective secure and privacy-preserving OSNs. We hope that this work will motivate OSN researchers and developers to move forward with more creative design of OSNs without compromising users' data security and privacy.

Adrienne Felt et. al. [3] enforced for third-party applications. Using the privacy-by-proxy approach, a social networking site has control over the application output and can support applications without compromising user data. Our design is motivated by how current Facebook applications (which were developed with an open, privacy-compromising interface) actually use information. Our findings indicate that a simple privacy preserving interface, combined with our privacy-byproxy approach is able to support nearly all existing

applications while providing privacy protection. Admittedly, open social network platforms are new and it is possible that a privacy-preserving interface would inhibit potentially valuable future applications more than is apparent from out study of current Facebook applications. There is an inherent tradeoff between protecting privacy, which requires limiting access to information, and providing a rich interface; our work seeks a compromise.

Leucio Antonio Cutillo et. al. [4] Online social networks currently are among the best accepted and most highly utilized networked applications on the Internet. Their immense user base, which by 2010 has exceeded 500 million distinct users, permits predicting that they will stay being one of the killer apps during the coming years. However, both their users and their providers have not learned to properly master their properties, and the vast number and severity of threats, as well as the plethora of reported attacks, underlines the importance of introducing and enforcing security measures, which are better than the rudimentary approaches that are implemented today.

III. SOFTWARE REQUIREMENTS ANALYSIS

Requirement analysis for web applications encompasses three major tasks: formulation, requirements gathering and analysis modeling. During formulation, the basic motivation and goals for the web application are identified, and the categories of users are defined. In the requirements gathering phase, the content and functional requirements are listed and interaction scenarios written from end-user's point-of-view are developed. This intent is to establish a basic understanding of why the web application is built, who will use it, and what problems it will solve for its users.

3.1 Existing System with Limitations

- It is time consuming process as the user has to type the dbase commands. He has to remember all the commands which are difficult.
- It is limited to a single system.
- A user who wants only to have some information has to contact the administrator every time.

3.2 Proposed System Features

- User friendliness is provided in the application with various controls.
- The system makes the overall project management much easier and flexible.
- It can be accessed over the internet.
- Vast amount of data can be stored.
- There is no risk of data mismanagement at any level while the project development is under process.
- Relationship between the administrator, owner/developer and subcontractor can be maintained very easily.
- It provides high level of security using different protocols like https etc.

3.3 Proposed System

The proposed system is an social networking allowing the users to interact with each other and exchange their views. This paper also enables the users to see the details of their friends upload their own photographs, add their friends, leave a scrap & send testimonials.

1. The paper's objective is to enable users to communicate with other people.
2. It allows the user to search for friends.
3. This website provides user the ability to upload the photographs.
4. It also enables the user to leave the scraps & send the testimonials.

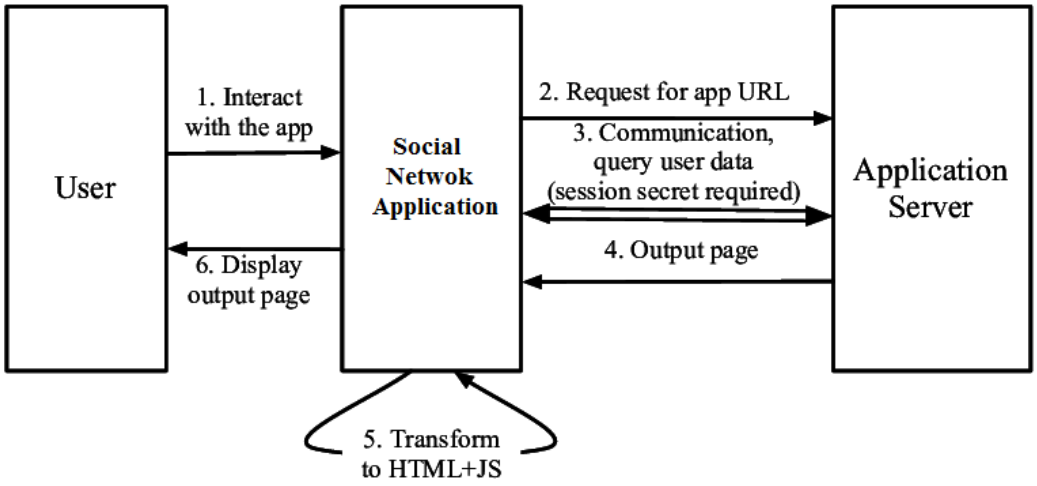


Figure 1: Architecture of Proposed system

3.4 Flowchart and Class diagram of Proposed System

Flowchart

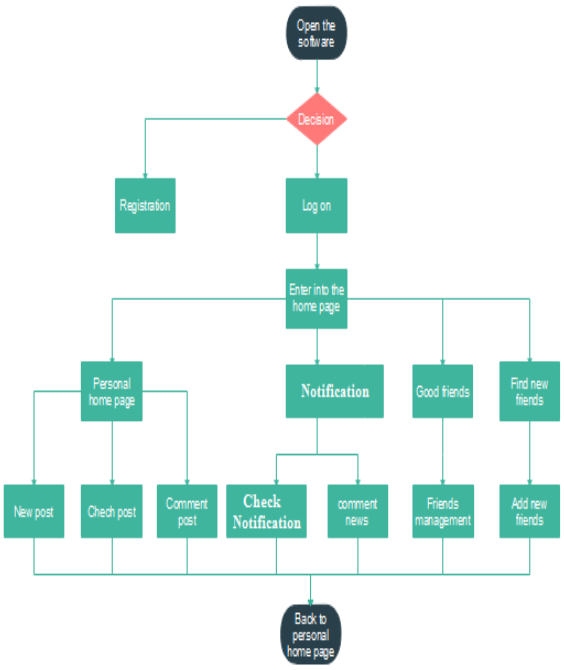


Figure 2: Flow chart of proposed system

Class diagram

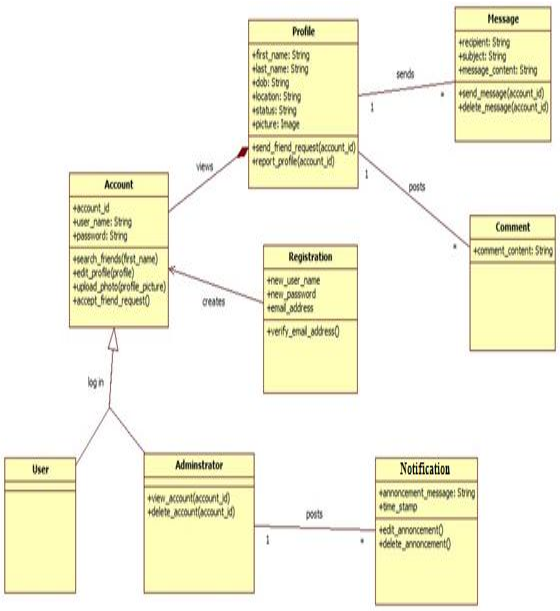


Figure 3: Class diagram of proposed system

3.5 Sequence Diagram

- An interaction diagram shows an interaction, consisting of a set of objects and their relationships, including the messages that may be dispatched among them.
- A sequence diagram is an interaction diagram that emphasizes the time ordering of messages.
- Graphically, a sequence diagram is a table that shows objects arranged along x-axis and messages, ordered in increasing time, along the y-axis.

Sequence diagram

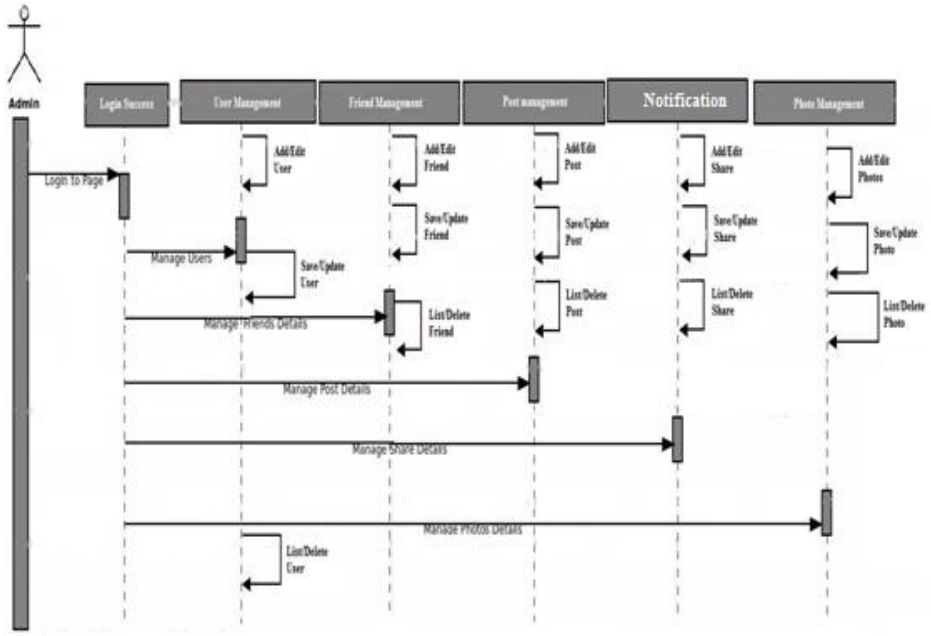


Figure 4: Class diagram

3.6 Use Case Diagram

Admin Use Case

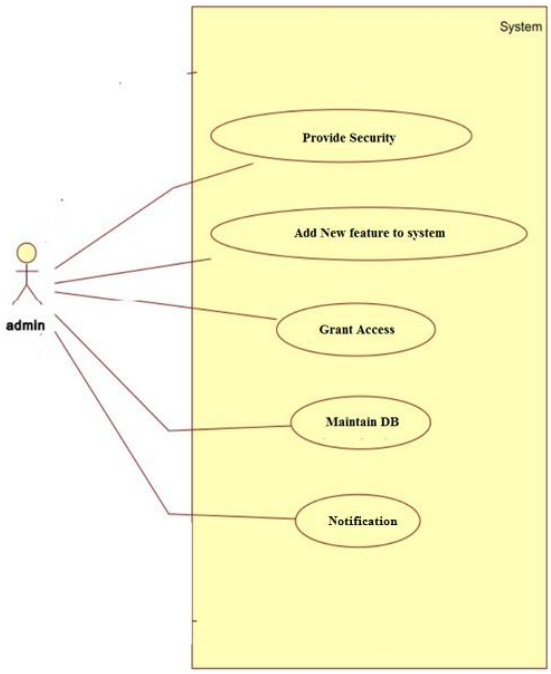


Figure 5: Admin use case

User use case

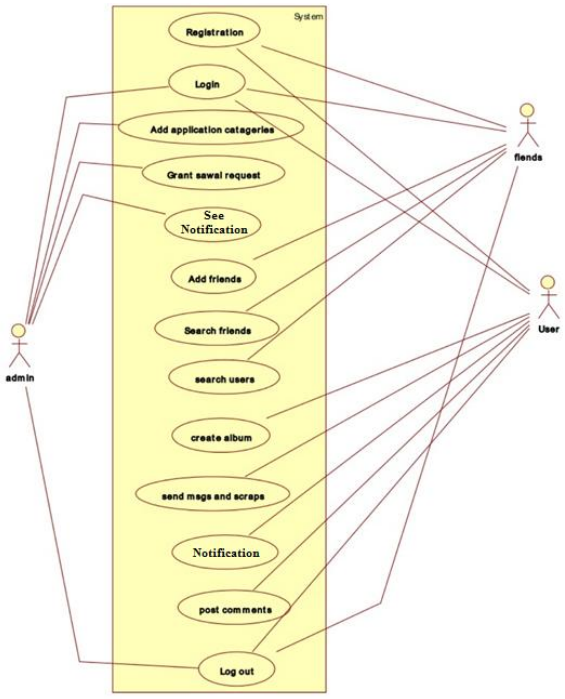


Figure 6: User use case

3.7 Control Flow Diagrams

Activity diagrams

An activity diagram shows the flow from activity to activity. An activity is an ongoing non- atomic execution within a state machine.

Activities ultimately result in some action, which is made up of executable atomic computations that result in a change in state of the system or the return of a value.

Login Process

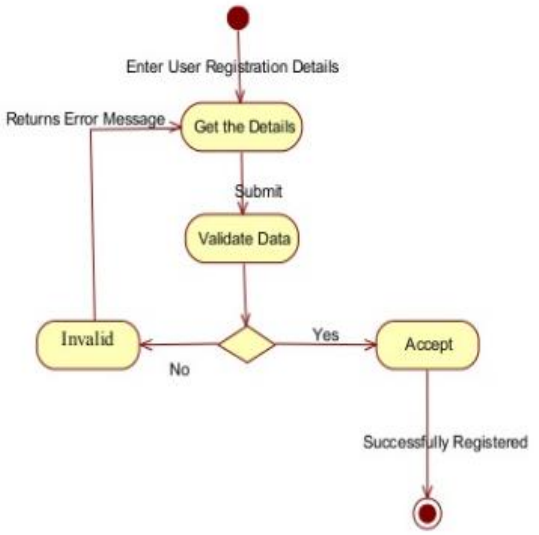


Figure 7: Control Flow Diagrams of Login Process

Registration Process

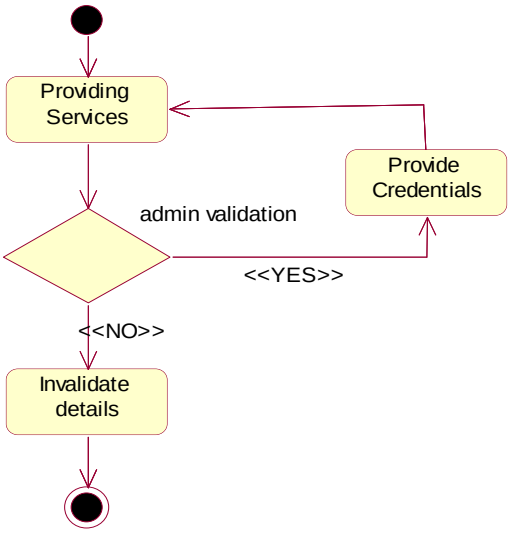


Figure 5: Control Flow Diagrams of Registration Process

Component diagram

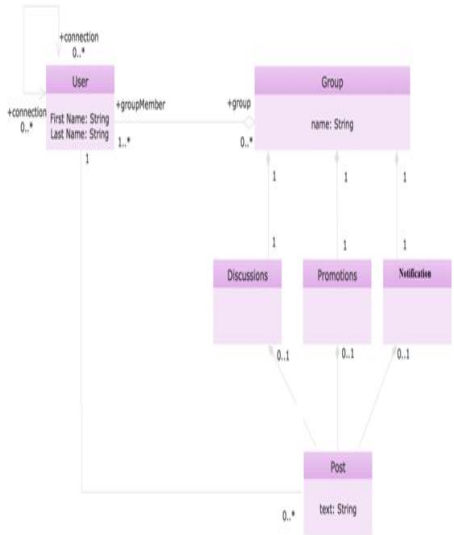
Component is a physical Part of a system that conforms to and provides realization of set of interfaces. A component is a self contained unit that encapsulates state and behavior of various set of classifiers. A component provides set of classes and interfaces with some functionality and GUI interfaces which may be required to in several services.

Deployment diagram

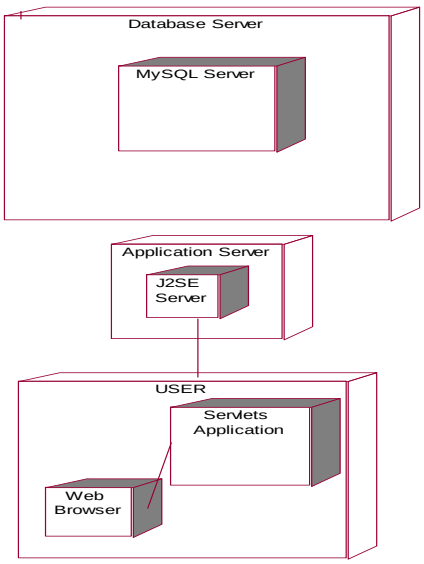
A deployment diagram is a diagram that shows the configuration of run time processing nodes and the components that live on them.

Graphically, a deployment diagram is collection of vertices and arcs.

Component diagram



Deployment diagram



IV. TEST SPECIFICATION

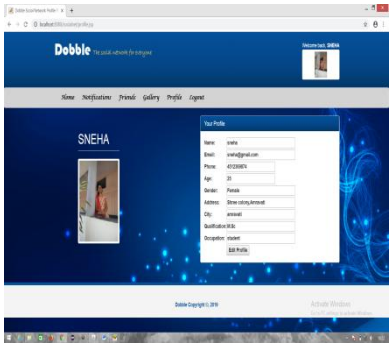
This section describes the overall testing strategy and the project management issues that are required to properly execute effective tests. We are testing the paper "Privacy Preserving and Data Integrity in Social Networking" which aims is to build an interaction between admin, Staff and the students. A system that will be able to manage the student result data of a college and provide easy access to the same. We are performing testing for different forms like User Registration, Search result, Add Post, Notification. Testing Strategy are

Unit Testing, Components for unit testing, Integration Testing, Validation testing, High Order Testing, Testing resources and staffing.

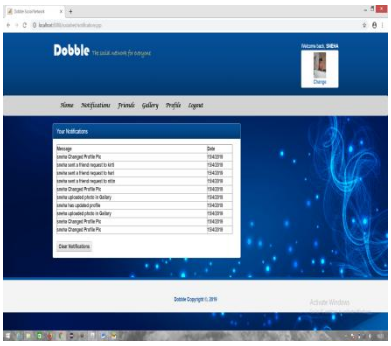
V. RESULT AND DISCUSSION

Home page

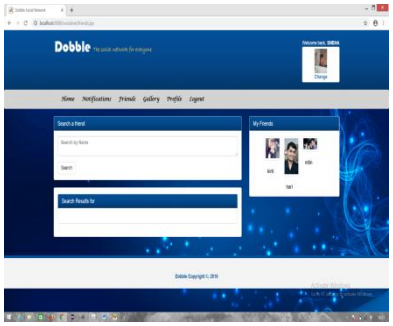
User Profile



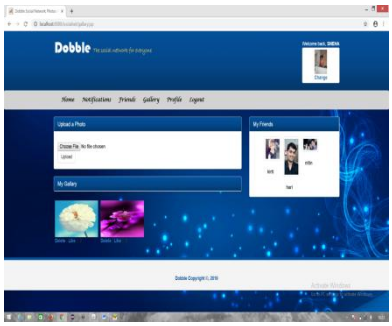
Notification



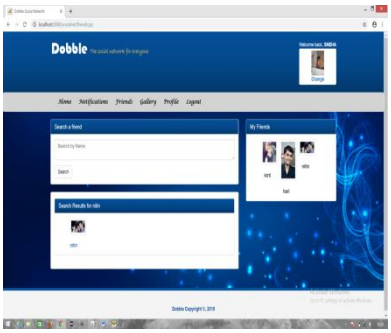
Friends



List Gallery



Friends search result



Friend profile

VI. CONCLUSION AND FUTURE SCOPE

Conclusion **:**The goal of the system is achieved and difficulties are solved. The paper application is built such that it is user friendly. Analysis of the scoring system it shows by the grade wise result of individual subject and final result also display grade wise. Depending on its range of marks. The paper application can be easily used in college for college result analysis of student. It reduces time which required for manual calculation. This system helps to calculate result fast so it optimizes the manpower.

Future Scope: In this paper data used to be inserted manually to analyze result. But, in future the paper application supports excel (.xlsx) files for extraction of data. The future scope is that data can be fetched, parsed in other formats like doc, csv, odt , etc .

REFERENCES

[1]. Ariel J. Feldman, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten, "Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider"
[2]. Chi Zhang and Jinyuan Sun, University of Florida Xiaoyan Zhu, Yuguang Fang, "Privacy and Security for Online Social Networks: Challenges and Opportunities", IEEE Network July/August 2010
[3]. Adrienne Felt, David Evans. "Privacy Protection for Social Networking Platforms",
[4]. Leucio Antonio Cutillo1, Mark Manulis2, and Thorsten Strufe, "Security and Privacy in Online Social Networks",
[5]. Chew Li Sa, Dayang Hanani bt. Abang Ibrahim,Emmy Dahliana Hossain,Mohammad bin Hossin, Student performance analysis system (SPAS),2015.
[6]. Ishwank Singh,A Sai Sabitha, Abhay Bansal, Student performance analysis using clustering algorithm,2016.

[7]. Sérgio Gonçalves ,Davide Carneiro , Javier Alfonso ,Florentino Fdez-Riverola, Paulo Novais ,Analysis of student's context in e-Learning, 2015.
[8]. Nada Elgendy,Ahmed Elragal,Big Data Analytics: A Literature Review Paper,2014.
[9]. Amar, J. S. and Mohini, B. (2009). Single Portal for Integrated Examination System. Journal of Emerging technologies in e-Governance, (pp. 287-293).
[10]. Anigbogu, S.O. (2000). Computer Application and Operation, (1st ed., Vol. 1, No.2, pp. 30-39). Awka: Optimum Press.
[11]. Barrett, S. (1999). Information's Systems: An Exploration of Factors Influencing Effective Use. Journal of Research on Computing in Education, (Vol. 32, No. 1, pp. 4-16).
[12]. Brian, P. (2009). Oracle Database 11g: PL/SQL Fundamentals, (Vol. 10). Redwood City, California: Oracle University Press.
[13]. Ekpenyong, M. E. (2008). A Real-Time IKBS for Students' Results Computation. International Journal of Physical Sciences, (Vol. 20, No. 3).
[14]. [online] Available: https://en.wikipedia.org/wiki/Student_information_system
[15]. [online] Available: https://en.wikipedia.org/wiki/Systems_analysis